Bayerischer Landtag
12. Wahlperiode

Drucksache 12/4144

05. 12. 91

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 14

München, 5. Dezember 1991

An den
Präsidenten
des Bayerischen Landtags
Herrn Dr. Wilhelm Vorndran
München

Dreizehnter Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrter Herr Landtagspräsident!

In der Anlage übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes den dreizehnten Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Dreizehnter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1991

Inhaltsübersicht

		Seite
1.	**Vorbemerkungen**	5
1.1	Kontrolltätigkeit	5
1.2	Datenschutz in Bayern gewährleistet	5
1.3	Inhalt und Schwerpunkte des 13. Tätigkeitsberichts	5
1.4	Neufassung des Bayerischen Datenschutzgesetzes	6
1.5	Geschäftsstelle	6
1.6	Befugnisse des Landesbeauftragten bei der Beratung des Haushalts	6
1.7	Datenschutz in Europa	7
1.8	Datenschutz — Innere Sicherheit — Organisierte Kriminalität	7
2.	**Gesundheitswesen**	7
2.1	Honorarabrechnung für ambulante Privatpatienten — Arztgeheimnis	7
2.2	Datenschutzkontrolle in einem Gesundheitsamt	9
2.3	Datenschutzkontrolle beim Bayer. Roten Kreuz	9
2.4	Meldung von Patientendaten an Krebsregister (anonymisierte Führung von Krebsregistern)	10
2.5	Anonymer unverknüpfbarer HIV-Test (AUT)	11
2.6	Automatisierte Krankendokumentation mit dem Verfahren KLIMACS	11
2.7	Fernwartung eines Klinik-DV-Systems	12
3.	**Sozialbehörden**	12
3.1	Bürgereingaben	12
3.2	Besetzung der Gremien von Betriebskrankenkassen	12
3.3	Hinweis der Krankenkasse an Arbeitgeber bei Schadensersatzanspruch	13
3.4	Datenübermittlung von Krankenkassen an die Sozialhilfeverwaltung	13

3.5 Weiterleitung von Kindererziehungsleistungen an Heimbewohnerinnen durch die Sozialämter 14
3.6 Krankenkassenzugehörigkeit der Mitgliedsbetriebe einer Handwerksinnung 14

4. Polizei 15
4.1 Zur Lage des Datenschutzes 15
4.2 Schwerpunkte 15
4.3 Erfahrungen mit dem neuen Polizeiaufgabengesetz (PAG) 16
4.4 Allgemeine Prüfungen 17
4.4.1 Kriminalaktennachweis (KAN) 17
4.5 Polizeipräsidium München 18
4.5.1 Anordnungen von besonderen Mitteln der Datenerhebung 18
4.5.2 Kriminalpolizeilicher Aktennachweis (KAN) 18
4.5.3 Datei in einem Arbeitsplatzcomputer 18
4.5.4 Verschiedene Karteien 18
4.6 Bayerisches Landeskriminalamt (BLKA) 18
4.7. Kriminalaktennachweis (KAN) und Polizeiaufgabengesetz (PAG) 19
4.7.1 Reduzierung der KAN-Speicherungen 19
4.7.2 Verkürzung der Aussonderungsprüffristen 20
4.7.3 Einschränkung der Fristenverlängerungsautomatik 20
4.8 Arbeitsdatei PIOS Innere Sicherheit (APIS) 20
4.8.1 Abschaffung von APIS 21
4.8.2 Reduzierung der Speicherungen in APIS 21
4.8.3 Erweiterung von APIS 22
4.9 Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung — Verbrechensbekämpfung" (PSV) 22
4.9.1 Dateibeschreibung 22
4.9,2 Datenschutzrechtliche Bewertung der PSV 23
4.10 Datei „Gewalttäter Sport" 24
4.11 Datei „Straftäter bei Sportveranstaltungen und gewalttätige Jugendgruppen" 26
4.12 Berücksichtigung des Verfahrensausgangs 26
4.13 Speicherung von Schwangeren wegen strafbarer Abtreibung 27
4.14 Bürgereingaben 27

5. Verfassungsschutz 29
5.1 Vorbemerkung 29
5.2 Existenzberechtigung des Verfassungsschutzes 29
5.3 Behinderung des Verfassungsschutzes durch den Datenschutz 29
5.4 Zusammenfassende Feststellung 29
5.5 Generelle Prüfung 1991 29
5.6 Bürgereingaben 30
5.7 Interne Arbeitsanweisungen 30
5.8 Datei „Karteiüberwachung" 31
5.9 Überwachung der Partei des demokratischen Sozialismus (PDS) in Bayern 31
5.10 Kontrolle der Anwendungen nachrichtendienstlicher Mittel 32

6. Justiz 32
6.1 Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) 32
6.2 Novellierung des Strafvollzugsgesetzes 34
6.3 Justizmitteilungsgesetz (JuMiG) 34
6.4 Kontrolle einer Staatsanwaltschaft 35
6.5 Kontrolle einer Justizvollzugsanstalt 36
6.5.1 Manuelle Karteien 36
6.5.2 Zugriff zu Personalakten 37
6.5.3 Wahrnehmungsbögen 37
6.5.4 Automatisierte Verfahren 37
6.6 Datenschutz im gerichtlichen Verfahren 38
6.6.1 Übersendung psychiatrischer Gutachten an den Prozeßgegner 38
6.6.2 Wiedergabe psychiatrischer Gutachten in gerichtlichen Entscheidungen 38
6.7 Datenschutz im Notariat 39

7. Regierungen, Landkreise, Städte und Gemeinden 40
7.1 Vergabe von Erschließungsbeitragsarbeiten an Privatunternehmen 40
7.2 Prüfung einer Großstadt 40
7.3 Prüfung eines Landratsamtes 41
7.4 Prüfung eines Wasserwirtschaftsamtes 41
7.5 Veröffentlichung eines Untersuchungsberichts 42
7.6 Mieterinformationen in Stadterneuerungsgebieten 42

7.7 Betretungsrecht eines Kontrolleurs der Stadtwerke 42
7.8 Weitergabe von Daten über Einkommensverhältnisse des Mieters an den Vermieter im Zusammenhang mit der Erhebung einer Ausgleichszahlung nach § 7 Wohnungsbindungsgesetz 42
7.9 Übermittlung der Daten kommunaler Mandatsträger an die Handwerkskammern 43
7.10 Online-Zugriff der Rechnungsprüfungsämter auf Daten der Verwaltung 43
7.11 Auskunft aus der Kaufpreissammlung 43
7.12 Speicherung von gemeindlichen Sitzungsvorlagen in einem Privat-PC durch ein Mitglied des Gemeinderates 44
7.13 Umfrage zum Einkaufsverhalten der Bürger 44
7.14 Betriebsbefragung in der Landwirtschaft und im Gartenbau 45

8. Einwohnermeldewesen 45
8.1 Rechtliche Entwicklung 45
8.2 Prüfungen 45
8.3 Datenschutz-Verstöße und Probleme des Melderechts — Einzelfälle . 46
8.3.1 Gesetzlicher Vertreter im Datensatz eines polizeilich Gesuchten 46
8.3.2 Meldedatenübermittlung an das Jugendamt zur Vaterschaftsfeststellung 46
8.3.3 Wähleradressen an politische Parteien und Wählergruppen 46
8.3.4 Datenübermittlung an Adreßbuchverlage 47
8.3.5 Gruppenauskünfte 47
8.3.6 Widerspruchsrechte der Bürger nach dem Bayer. Meldegesetz (MeldeG) 48
8.3.7 Adressenübermittlung an die Polizei zur Nachwuchswerbung für den Polizeivollzugsdienst 48

9. Ausländerwesen 48
9.1 Neues Ausländergesetz 48
9.2 Entwurf eines Ausländerzentralregistergesetzes 49
9.3 ED-Behandlung von Asylbewerbern 50

10. Steuerverwaltung 51
10.1 Änderungen im Datenschutzrecht für die Steuerverwaltung 51
10.2 Bundesverfassungsgericht: Besteuerung von Kapitaleinkünften 51
10.3 Prüfung bei einem Finanzamt 52
10.4 Neue Lohnsteuerkarte bei Arbeitgeberwechsel 53

11. Vermessungswesen 53
11.1 Automatisiertes Liegenschaftsbuch (ALB) 53
11.1.1 Einsicht und Auskunft 53
11.1.2 Zusätzliche Daten 54
11.1.3 Gesamtkonzept 54
11.2 Prüfung eines Vermessungsamts . . 54

12. Personalwesen 55
12.1 Mitbestimmung des Personalrates . 55
12.2 Grundsätze zum Datenschutz der Arbeitnehmer im öffentlichen Dienst 55
12.3 Telefongesprächsdatenerfassung . . 55
12.4 Eigene Rechtsstellung für Angehörige im Beihilfeverfahren 56
12.5 Verarbeitung personenbezogener Personaldaten durch Gewerbeaufsichtsämter 56
12.6 Informationspflicht des örtlichen Personalrats gegenüber dem Vertrauensmann der Schwerbehinderten 56
12.7 Aufbewahrung polizeiärztlicher Gutachten 57

13. Gewerbe und Handwerk 57
13.1 Datenschutzprüfung bei einer Handwerkskammer 57
13.2 Datenerhebung für die Eintragung in die Handwerksrolle 58
13.3 Datenübermittlung an Berufsvereinigung im Rahmen von Ausnahmebewilligungsverfahren 58

14. Landwirtschaft 59
14.1 Prüfung eines Amtes für Landwirtschaft 59

15. Statistik 59
15.1 Volkszählung 1987 59
15.2 Fragebogen bei der Erstellung der Einzelhandelsstatistik 60
15.3 Faktische Anonymisierung bei Übermittlung von Einzelangaben von Statistikämtern an Hochschulen 60

15.4 Weitergabe der Viehzählungslisten durch Gemeinden an Veterinärämter für tierseuchenrechtliche Maßnahmen 61

15.5 Viehzählung — Statistikgeheimnis, Aufbewahrung von Viehzählungsunterlagen 61

16. Schulwesen 61

16.1 Verwendung von Echtdaten in der Landwirtschaftsschule 61

16.2 Hinweis auf die Aufnahmeprüfung im Notenbogen der Abschlußklasse 62

16.3 Offenbarung von Sozialhilfedaten an Fachoberschüler 62

16.4 Meldung von Schulunfällen an den Bayerischen Gemeindeunfallversicherungsverband 63

17. Hochschule 63

18. Archiv und Forschung 63

18.1 Prüfung des Landesamts für Denkmalpflege 63

18.2 Veröffentlichung von Zuschüssen aus Mitteln des Entschädigungsfonds nach dem Denkmalschutzgesetz 64

18.3 Datenschutz bei Dissertationen . . . 64

18.4 Standesamtswesen — genealogische Forschung 65

19. Umweltfragen 65

20. Verkehrswesen 66

20.1 Speicherung von Unschuldigen in „Schwarzfahrerdateien“ 66

20.2 Auskünfte der Kraftfahrzeugzulassungsstellen an Rundfunkanstalten . 66

20.3 Einheitliche Notrufnummer in Europa 67

20.4 Zentrales Verkehrsinformationssystem (ZEVIS) 67

21. Medien 69

21.1 Medien und Datenschutz 69

21.2 Rundfunkanstalten des Bundes . . . 69

21.3 Datenschutz bei der Presse 69

21.4 Bayerischer Rundfunk 70

21.5 Entwurf des Bayerischen Mediengesetzes 70

21.6 Staatsvertrag über den Rundfunk im vereinten Deutschland 71

21.7 Prüfung einer Kabelgesellschaft . . . 72

21.8 Datenschutz in der Telekommunikation 73

22. Technischer und organisatorischer Bereich 74

22.1 Fortentwicklung der Datensicherheit 74

22.1.1 Anforderungen an sichere DV-Systeme 75

22.1.2 Sicherheitsanforderungen bei der Vernetzung von Personal Computern 76

22.1.3 Einsatz der Chipkarte 78

22.2 Prüfungstätigkeit 78

22.2.1 Kontrolle und Beratung 78

22.2.2 Ergebnisse der Kontrolltätigkeit . . 79

22.2.3 Datenverarbeitung bei der Steuerverwaltung 80

22.3 Technische Einzelprobleme 81

22.3.1 Datensicherheit bei Teletex 81

22.3.2 Betrieb von Telekommunikationsanlagen 81

22.3.3 Version 10 von BS2000 81

22.3.4 Überspannungsschutz und unterbrechungsfreie Stromversorgung 82

22.3.5 Datensicherheit beim APC-Einsatz . 82

22.3.6 Abschottung der statistischen Datenverarbeitung 83

22.3.7 Plausibilitätsprüfungen 83

22.3.8 Software-Entwicklung durch private Dritte 84

22.3.9 Zusammenarbeit mit der AKDB . . 84

23. Datenschutzregister 85

24. Datenschutz beim Bayer. Rundfunk (BR) 85

25. Der Beirat 87

26. Konferenz der Datenschutzbeauftragten des Bundes und der Länder . . 88

Anlage 1: Beschluß der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29.01.1991 zum Vorschlag der Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten 88

Anlage 2: Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes 89

1. Vorbemerkungen

1.1 Kontrolltätigkeit

Der Schwerpunkt meiner Tätigkeit lag im Berichtszeitraum wieder bei der Kontrolle bayerischer Behörden. **Allgemeine Kontrollen** habe ich durchgeführt bei einer Handwerkskammer, einem Amt für Landwirtschaft, dem Landwirtschaftsministerium, einem Gesundheitsamt, dem Bayer. Roten Kreuz (Präsidium und einem Kreisverband), einer Staatsanwaltschaft, einer Justizvollzugsanstalt, dem Landeskriminalamt, einem Polizeipräsidium, neun Polizeidirektionen, dem Landesamt für Verfassungsschutz, einem Vermessungsamt, einer Kabelgesellschaft, sieben Städten, einem Landratsamt, einem Wasserwirtschaftsamt und dem Landesamt für Denkmalpflege.

Ergänzt wurden die allgemeinen Kontrollen durch zahlreiche Überprüfungen von Behörden aufgrund von Eingaben, Beschwerden und Presseberichten. Hinzu kommen technisch-organisatorische Kontrollen bei 19 Rechenzentren und Betreibern kleinerer Datenverarbeitungsanlagen sowie 24 Besuche bei Behörden zur Überprüfung der datenschutzgerechten Entsorgung von Datenträgern.

1.2 Datenschutz in Bayern gewährleistet

Wie in den Vorjahren kann ich auf der Grundlage der durchgeführten Kontrollen und zahlreicher weiterer Behördenkontakte feststellen, daß der Datenschutz in Bayern grundsätzlich gewährleistet ist.

1.3 Inhalt und Schwerpunkte des 13. Tätigkeitsberichts

Dieser Bericht kann aus Platzgründen wieder nur eine Auswahl aus meiner Tätigkeit im Berichtszeitraum enthalten. Den Schwerpunkt bilden die Ergebnisse der durchgeführten Datenschutzkontrollen. Auf Anfragen von Behörden und Bürgern waren wieder zahlreiche Zweifelsfragen über die Reichweite datenschutzrechtlicher Vorschriften zu klären. Soweit die Stellungnahmen von allgemeinem Interesse sind, habe ich sie im Bericht wiedergegeben. Zu einer Reihe von Gesetzgebungsvorhaben, Richtlinien und Dienstanweisungen, die den Datenschutz betreffen, habe ich Stellung genommen.

- Im Vordergrund standen meine Bemühungen um einen **angemessenen Datenschutz im Sicherheitsbereich**. Neben allgemeinen Datenschutzkontrollen, deren Ergebnisse wiedergegeben sind, ging es vor allem darum, die Errichtungsanordnungen und Dienstanweisungen der Polizei und des Verfassungsschutzes an die Neufassungen des Polizeiaufgabengesetzes und des Bayerischen Verfassungsschutzgesetzes anzupassen.

  Im Mittelpunkt stand dabei der **Kriminalaktennachweis**: Er muß noch weiter „entrümpelt" werden. Straftaten von geringerer Bedeutung müssen rascher aus der Datei gelöscht werden.

  Die Datei **„Polizeiliche Sachbearbeitung/Vorgangsverwaltung — Verbrechensbekämpfung"**, welche die Grundlage des Informationssystems der Bayerischen Polizei werden soll, muß in räumlicher und organisatorischer Hinsicht so ausgestaltet werden, daß bei aller wünschenswerten Effektivität der Verbrechensbekämpfung der Grundsatz der Erforderlichkeit polizeilicher Datenspeicherungen strikt beachtet und Datenmißbräuche möglichst ausgeschlossen werden.

  Die öffentliche Diskussion um die **Staatsschutzdatei APIS** wurde fortgesetzt, teils in Richtung Einschränkung, teils in Richtung Ausweitung, insbesondere Verlängerung der Speicherfristen.

  Zwischen Polizei und Datenschutz sowie unter den Datenschutzbeauftragten intensiv erörtert wurden Pläne zur Errichtung einer **Verbunddatei „Gewalttäter Sport"** zur frühzeitigen und wirksamen Bekämpfung gewalttätiger Ausschreitungen im Zusammenhang mit Sportveranstaltungen. Unter bestimmten Voraussetzungen wie überörtliches Auftreten der Gewalttäter kann diese Datei ein brauchbares Hilfsinstrument für polizeiliche Entscheidungen sein. Ängstliche Zweifel an der Eignung einer Datei „Gewalttäter Sport" sind angesichts verheerender Ausschreitungen von deutschen „Fußball-Fans" in Brüssel unangebracht.

- Im **Gesundheitsbereich** hat der Bundesgerichtshof mit der Entscheidung vom 10.7.1991 die herausragende Bedeutung der ärztlichen Schweigepflicht betont und der **schleichenden Aushöhlung des Arztgeheimnisses** des Patienten Schranken gesetzt.

  Bei der Nutzung von Patientendaten durch Dritte (Krebsregister, anonymer unverknüpfbarer HIV-Test) achtete ich darauf, daß nur **anonymisierte** Daten den ärztlichen Bereich verlassen.

- Im **Justizbereich** hatte ich den Gesetzentwurf des Bundesrats zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der **organisierten Kriminalität** zu bewerten, der von fast allen Bundesländern unterstützt wird. Während ich die vorgeschlagenen Bestimmungen zu Rasterfahndung, Einsatz verdeckter Mittel und verdeckter Ermittler, polizeiliche Beobachtung etc. angesichts der **dramatischen Bedrohung** der deutschen und europäischen Gesellschaft durch die organisierte Kriminalität im großen und ganzen für angemessen halte, lehnt die Mehrzahl der Datenschutzbeauftragten den Gesetzentwurf als zu weitgehenden Eingriff in das informationelle Selbstbestimmungsrecht ab.

Ungelöst sind die Probleme, die sich daraus ergeben, daß in Gerichtsverfahren die über Beteiligte erstellten **ärztlichen Gutachten** aufgrund der Anforderungen der Gerichte immer tiefer in die Intimsphäre eindringen, und auf diesem Weg den übrigen Prozeßbeteiligten Einblick in intimste Angelegenheiten gewährt wird. Die Gewähr rechtlichen Gehörs und die Wahrheitsfindung vor Gericht haben vor der **Würde des Menschen** Halt zu machen.

- Zur **Ermittlung der Vaterschaft** eines unehelichen Kindes wollte ein Amtspfleger bei einem Jugendamt von den Einwohnermeldeämtern eines größeren Einzugsbereichs die Namen und Adressen aller Männer mit einem bestimmten Vornamen im Alter von 28 bis 33 Jahren übermittelt erhalten. Bei allem Verständnis für das Anliegen, den Vater des Kindes festzustellen, habe ich gegen diese Art von „Rasterfahndung" erhebliche datenschutzrechtliche Bedenken.

- Die zunehmende Abhängigkeit der Behörden von einer funktionierenden Datenverarbeitung und die Speicherung besonders sensibler Informationen machen es dringend erforderlich, zum Schutz der Datenverarbeitung vor Mißbrauch und Störungen die auf dem Markt verfügbaren **Sicherheitseinrichtungen wie Chipkarte und Sicherheitssoftware** stärker als bisher einzusetzen. Das gilt auch für die individuelle Datenverarbeitung mit Personal Computern. Besonders ist darauf zu achten, daß neue Software vor ihrem Einsatz auf **Virenbefall** zu überprüfen ist. Ein Virenbefall kann die gesamte Datenverarbeitung lahmlegen und zur Verfälschung und zum Verlust der Daten führen. Bei der **Entsorgung von Papierunterlagen** lassen es manche Behörden nach wie vor an der gebotenen Sorgfalt fehlen. Unterlagen mit Sozialdaten lagen in jedermann zugänglichen Müllcontainern.

1.4 Neufassung des Bayerischen Datenschutzgesetzes

Nachdem das neue Bundesdatenschutzgesetz (BDSG) zum 1. Juni 1991 in Kraft getreten ist, bereitet das Staatsministerium des Innern eine Neufassung des Bayerischen Datenschutzgesetzes vor. Ziel der Novelle muß es dabei insbesondere sein, die Forderungen des Bundesverfassungsgerichts im Urteil zum Volkszählungsgesetz und in späteren Entscheidungen in bayerisches Recht umzusetzen.

1.5 Geschäftsstelle

Aufgaben und Arbeitsbelastung der Geschäftsstelle haben infolge vermehrter bereichsspezifischer detaillierter Regelungen des Datenschutzes sowie als Folge der beschleunigten Ausweitung der automatisierten Datenverarbeitung stark zugenommen. Der Bayerische Landtag hat dieser gewachsenen Bedeutung des institutionellen Datenschutzes Rechnung getragen und im Doppelhaushalt 1991/92 trotz des Zwangs zum Sparen die angemessene Ausweitung der Geschäftsstelle gebilligt. Diese zusätzliche Personalausstattung versetzt mich in die Lage, insbesondere den stark gewachsenen Kontrollaufgaben bei der Polizei als Folge der starken Ausweitung der automatisierten Datenverarbeitung nachzukommen.

Im Berichtszeitraum mußte ich wegen des durch die Wiedervereinigung ausgelösten Personalmehrbedarfs im Beitrittsgebiet allerdings mit weniger Personal auskommen. Der Leiter des für den Datenschutz bei Polizei, Verfassungschutz und Justiz zuständigen Referats wurde zum Stellvertreter des Bundesbeauftragten für die Stasi-Akten berufen. Ein Mitarbeiter wurde zum Aufbau des Datenschutzes nach Thüringen abgeordnet und ein anderer leistet Verwaltungshilfe in Sachsen. Die vorübergehende personelle Schwächung der Geschäftsstelle mußte jedoch hingenommen werden, da der Aufbau einer funktionierenden Verwaltung in den östlichen Bundesländern vorrangig unterstützt werden muß.

1.6 Befugnisse des Landesbeauftragten bei der Beratung des Haushalts

Während der Landtagsberatungen zu den Personal- und Sachmitteln des Landesbeauftragten für den Datenschutz ist es zwischen dem Ministerpräsidenten und dem Landesbeauftragten zu unterschiedlichen Auffassungen in der Frage gekommen, unter welchen Voraussetzungen sich der Landesbeauftragte an Landtag und Senat wenden darf, wenn er der Auffassung ist, daß die von der Staatsregierung im Haushaltsentwurf vorgesehene Sach- und Personalausstattung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben nicht ausreicht.

Meine Personal- und Sachmittelanmeldungen im Rahmen des Aufstellungsverfahrens für den Staatshaushalt 1991/1992 waren aus meiner Sicht nicht im notwendigen Umfang berücksichtigt worden. Ich hatte mich deshalb nach intensiven, aber vergeblichen Bemühungen bei der Staatskanzlei unmittelbar an den Senat und dann auch an den Haushaltsausschuß des Landtags mit der Bitte um Unterstützung meines Anliegens gewandt.

Nach der Beratung im Haushaltsausschuß des Landtags beanstandete der Ministerpräsident mein Vorgehen. Er vertrat ebenso wie vorher die Staatskanzlei die Auffassung, daß die in Art. 27 des Bayerischen Datenschutzgesetzes festgelegte Unabhängigkeit des Landesbeauftragten keine Sonderstellung im parlamentarischen Verfahren für die Aufstellung des Staatshaushalts einräumt. Dadurch sah ich meine Befugnis in Frage gestellt, mich jederzeit an den Landtag und den Senat zu wenden, wenn ich es als Landesbeauftragter für den Datenschutz für erforderlich halte. In einem Schreiben an den Ministerpräsidenten habe ich die Auffassung vertreten, daß die Unabhän-

gigkeit des Landesbeauftragten für den Datenschutz und seine Verantwortung gegenüber dem Bayerischen Landtag, mit dessen Zustimmung er ernannt worden sei, das Recht einschließe, sich auch ohne Genehmigung durch den Ministerpräsidenten an einen Ausschuß des Landtags zu wenden. Das sei bei Gesetzesvorhaben bisher völlig unumstritten gewesen und könne bei den Beratungen des Haushaltsgesetzes nicht in Zweifel gezogen werden.

Der Ministerpräsident stellte nun klar, daß das Recht des Landesbeauftragten, sich jederzeit an das Parlament zu wenden, grundsätzlich unbestritten sei. Es sei im vorliegenden Fall darum gegangen, daß sich der Landesbeauftragte, wenn er sich im Haushaltsverfahren nicht durchsetzen könne, persönlich an den für den Haushalt der Staatskanzlei verantwortlichen Ministerpräsidenten wende, bevor er gegenüber Landtag und Senat vorstellig werde.

1.7 Datenschutz in Europa

Die EG-Kommission hat im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt. Die Datenschutzbeauftragten des Bundes und der Länder befaßten sich mit dem Vorschlag in einer Sonderkonferenz und faßten dazu den in **Anlage 1** wiedergegebenen Beschluß. Die Konferenz hat vor allem die Intention des Entwurfs positiv bewertet, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst **hohen Niveau** zu harmonisieren.

Es besteht jedoch Anlaß zur Sorge, daß der Rechtsausschuß des Europaparlaments die Richtlinie nicht unerheblich aufweichen wird.

1.8 Datenschutz — Innere Sicherheit — Organisierte Kriminalität

Der RAF-Mord an Treuhandchef C. Rohwedder am 1.4.1991 hat der Öffentlichkeit wieder einmal die verhängnisvollen Fahndungsdefizite der Sicherheitsbehörden gegenüber Terrorgruppen bewußt gemacht. Seit fast einem Jahrzehnt wurden gegen die RAF keine entscheidenden Fahndungserfolge mehr erzielt. In der öffentlichen Diskussion wurde hierfür auch der **Datenschutz verantwortlich** gemacht. Diesem Vorwurf muß sich der Datenschutz stellen. Niemand darf vor den offenkundigen Fahndungsdefiziten den Kopf in den Sand stecken und abwarten, bis sich die öffentliche Erregung nach dem letzten Mord gelegt hat, um dann wieder weitere Maximalforderungen zu erheben.

Nach meiner Auffassung müssen die Ursachen für die Fahndungsdefizite sorgfältig analysiert werden. Die Polizei sollte alle Maßnahmen nennen, die sie zur RAF-Bekämpfung für erfolgversprechend hält, die aber in der Vergangenheit wegen datenschutzrechtlicher Bedenken eingestellt oder nicht realisiert wurden. Nach dieser Bestandsaufnahme sollte unvoreingenommen geklärt werden, welche für geeignet gehaltenen Maßnahmen unter dem Gesichtspunkt des Datenschutzes zulässig und vertretbar erscheinen.

Ich bin keinesfalls der Meinung, daß man, wie der Bundesjustizminister, das Fehlen von Fahndungserfolgen mit der rechtsstaatlichen Ordnung in der Bundesrepublik erklären kann, welche die notwendigen Ermittlungsmethoden nicht zulasse. Genauso wenig kann ich mich der Ansicht anschließen, die Unkenntnis über den harten Kern der RAF sei der Preis für eine offene und freie Gesellschaft. Außer Zweifel steht selbstverständlich, daß unsere offene und freie Gesellschaft nicht der Bekämpfung des Terrorismus geopfert werden darf. Den Preis des Terrorismus müssen wir aber erst bezahlen, nachdem wirklich alle rechtsstaatlichen Mittel erschöpft sind. An diesem Punkt sind wir aber noch lange nicht angelangt.

Bei der Bewertung des Gesetzentwurfs des Bundesrats zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität zeigten sich unter den Datenschutzbeauftragten erhebliche Meinungsverschiedenheiten. Während sich nach meiner Überzeugung der Gesetzentwurf mit Erfolg bemüht, die Balance zwischen den Erfordernissen einer wirksamen Verbrechensbekämpfung und dem Schutz des einzelnen vor staatlichen Eingriffen zu wahren, warnt die Mehrheit der Datenschutzbeauftragten aus einem übersteigerten Rollenverständnis vor schwerwiegenden Eingriffen in die Bürgerrechte. Ich halte die weit überzogenen Forderungen für nicht verantwortbar, da sie überwiegend nur vordergründig die Freiheitsrechte der Bürger schützen, in Wirklichkeit aber der Freiheit und dem Schutz aller Bürger schaden würden. Datenschutz darf nicht zum Täterschutz werden.

2. Gesundheitswesen

2.1 Honorarabrechnung für ambulante Privatpatienten — Arztgeheimnis

Im Zusammenhang mit dem Vollzug des Nebentätigkeitsrechts hatte ich mich schon früher mit der Frage zu befassen, ob Krankenhausärzte der **Krankenhausverwaltung** personenbezogene Angaben über ambulante Behandlungen zur Kontrolle der Nebentätigkeitsabgaben offenbaren dürfen. Ich hatte damals die Anonymisierung der betreffenden Unterlagen für die Nebentätigkeitskontrolle gefordert (11. Tätigkeitsbericht Nr. 2.4).

Nunmehr hat der **Bundesgerichtshof** mit Urteil vom 10.7.1991 zur Weitergabe personenbezogener Patientendaten aus der ambulanten Privatbehandlung an eine **externe Verrechnungsstelle** Feststellungen getroffen, die in der von mir eingeschlagenen Richtung lie-

gen und auch für Krankenhausärzte von Bedeutung sind:

„Die Abtretung einer ärztlichen oder zahnärztlichen Honorarforderung an eine gewerbliche Verrechnungsstelle, die zum Zwecke der Rechnungserstellung und Einziehung unter Übergabe der Abrechnungsunterlagen erfolgt, ist wegen **Verletzung der ärztlichen Schweigepflicht** (§ 203 Abs. 1 Nr. 1 StGB) gem. § 134 BGB nichtig, wenn der Patient ihr nicht zugestimmt hat."

Aus dem Urteil ergeben sich Erkenntnisse für die Erstellung der **Privatliquidationen von Krankenhausärzten** nicht nur durch „gewerbliche" Verrechnungsstellen, sondern ganz generell durch andere Personen oder Stellen als die Sekretärin des Arztes (ärztliche Gehilfin). Der Bundesgerichtshof führt zunächst in der Begründung aus, daß zwar die Existenz berufsständischer „privatärztlicher Verrechnungsstellen" unter Privatpatienten heute wohl allgemein bekannt sei. Dies bedeute aber nicht, daß der Patient ohne weiteres davon ausgehen müsse, der Arzt, den er zur Behandlung aufsuche, lasse sein Honorar durch eine solche Stelle abrechnen und einziehen.

Nach Ansicht des BGH verdienen die häufig über intimste Geheimnisse des Patienten genaue Auskunft gebenden Abrechnungsunterlagen einen besonders wirksamen Schutz. Dieser sei grundsätzlich nur gewährleistet, wenn die Honorarabrechnung in einem von vornherein und sicher für den Patienten überschaubaren Bereich erfolge; das aber sei in aller Regel **allein die Praxis des behandelnden Arztes** einschließlich der für die Abrechnung zuständigen Mitarbeiter. Jedes Überschreiten der Grenzen dieses Bereichs stelle ein Offenbaren des dem Arzt anvertrauten Patientengeheimnisses dar, wobei es ohne Bedeutung sei, ob der Mitteilungsempfänger seinerseits — etwa als Arzt oder privatärztliche Verrechnungsstelle (§ 203 Abs. 1 Nr. 1 und 6 StGB) — der Schweigepflicht unterliege.

Zur Frage, ob eine **stillschweigende Einwilligung** des Patienten in die Offenbarung seiner Daten gegenüber der Verrechnungsstelle angenommen werden kann, führt der BGH aus, daß es zumindest fraglich erscheine, ob es hier stets ausreiche, wenn der Patient in Kenntnis einer entsprechenden Übung des behandelnden Arztes — etwa aufgrund eines schriftlichen Hinweises im Wartezimmer — dem nicht widerspreche. Der BGH weist darauf hin, daß es im Hinblick auf die ärztliche Schweigepflicht dem Arzt obliege, die Zustimmung des Patienten in eindeutiger und unmißverständlicher Weise einzuholen. Es sei grundsätzlich nicht Sache des Patienten, der Weitergabe seiner Daten zu widersprechen, um den Eindruck des stillschweigenden Einverständnisses zu vermeiden. Der BGH unterscheidet bei diesen Überlegungen nicht zwischen gewerblichen und privaten Verrechnungsstellen, sondern spricht allgemein von „externen Abrechnungsstellen".

Der BGH setzt sich auch mit der Frage auseinander, ob **sonstige Gründe** vorlagen, die das Offenbaren eines Patientengeheimnisses rechtfertigen könnten und führt aus, daß die Weitergabe von Behandlungsdaten an einen Dritten zum **Zwecke der Rechnungserstellung nicht zwingend erforderlich sei**. Der Einsatz elektronischer Datenverarbeitung erleichtere zwar die Honorarabrechnung in der ärztlichen Praxis erheblich. Soweit ein Arzt von der Möglichkeit externer Abrechnung Gebrauch mache, erfolge dies unter dem Gesichtspunkt einer Kosten-/Nutzenanalyse. Solche **wirtschaftlichen Erwägungen**, von denen die Durchsetzung des Honoraranspruchs nicht abhänge, vermöchten aber die Verletzung der ärztlichen Schweigepflicht unter keinen Umständen zu rechtfertigen.

Der BGH kommt zu dem Schluß, daß die Weitergabe der Abrechnungsunterlagen in dem zu entscheidenden Fall mithin schon wegen **Fehlens einer mündlichen oder konkludent erklärten Einwilligung** unzulässig war, so daß es für die Entscheidung nicht mehr darauf ankam, ob nach dem Bundesdatenschutzgesetz (§ 4 Abs. 2 Satz 2) sogar eine **schriftliche** Zustimmung erforderlich gewesen wäre. Auf unterschiedliche Äußerungen im Schrifttum zur Frage der Schriftform weist der BGH hin und läßt sie damit offen.

Für Krankenhausärzte ergibt sich daraus die Konsequenz, daß die vorherige Einwilligung des Patienten einzuholen ist, wenn die Abrechnung ambulanter Privatbehandlungen durch eine andere Person oder Stelle als die Arztsekretärin, insbesondere über die Krankenhausverwaltung oder eine externe Verrechnungsstelle durchgeführt werden soll. Eine **schriftliche** Einwilligung führt dabei zu klaren Verhältnissen. Ob bei **Aushang** eines eindeutigen schriftlichen Hinweises im Wartezimmer eine konkludente Einwilligung in Frage kommen kann, hat der BGH offengelassen, dürfte aber wegen des Beschäftigtseins des Patienten mit seiner Krankheit zu verneinen sein.

Im Zusammenhang mit der Abtretung der Honorarforderung an eine gewerbliche Verrechnungsstelle weist der BGH auch auf das Problem der **Zumutbarkeit** für den Patienten hin: Die Abtretung würde dazu führen, daß der Patient in einer Auseinandersetzung über die Berechtigung der Forderung gegenüber einem außerhalb des Arzt-/Patientenverhältnisses stehenden Dritten (der Verrechnungsstelle) Einwände gegen die Honorarabrechnung vorzubringen und dazu unter Umständen bisher unbekannte Einzelheiten aus der Vorgeschichte oder der Behandlung offenzulegen hätte. Derartiges sei dem Patienten aber — so die Urteilsbegründung — nicht zuzumuten.

Bei der Einschaltung einer externen Verrechnungsstelle ist es daher nicht allein mit der einwandfreien Einholung einer Einwilligung des Patienten getan.

Art und Umfang der Abrechnung durch einen Dritten müssen darauf Rücksicht nehmen, was dem Patienten in diesem Zusammenhang noch **zugemutet** werden kann.

2.2 Datenschutzkontrolle in einem Gesundheitsamt

Im Berichtszeitraum habe ich die Datenschutzkontrolle bei den Gesundheitsämtern fortgesetzt. Überprüft wurden
- die Führung von **Karteien**,
- die Datenerhebung im Zusammenhang mit **HIV-Tests** sowie
- die nach Art. 6 des Gesundheitsdienstgesetzes (GDG) gebotene organisatorische **Abschottung** der Aufgabenbereiche des Gesundheitsamtes.

Zentralkartei

In der Zentralkartei werden alle Personen registriert, die mit dem Gesundheitsamt Kontakt und deshalb hier eine Akte haben. Zu den die Person identifizierenden Angaben (Name, Anschrift, Geburtstag) wird jeweils die **Ziffer der Abteilung** des Gesundheitsamtes registriert, die mit der Person befaßt ist. Das überprüfte Gesundheitsamt ist freilich so organisiert, daß eine Abteilung sich **ausschließlich** mit Behinderten befaßt. Die auf der Karteikarte zur Person angegebene Ziffer weist damit nicht nur auf die damit befaßte Abteilung, sondern gleichzeitig auf die Art des gesundheitlichen Problems der Betroffenen hin.

Da nach Art. 6 des Gesundheitsdienstgesetzes Angaben, die Betroffene im Zusammenhang mit freiwilliger Beratung oder Begutachtung gemacht haben, grundsätzlich nicht für andere insbesondere hoheitliche Zwecke verwendet werden dürfen, habe ich schon früher in Übereinstimmung mit dem Staatsministerium des Innern gefordert, daß **in der Zentralkartei möglichst keine Hinweise auf die Art der Erkrankung** gespeichert werden, die aus einer solchen freiwilligen Beratung oder Begutachtung stammen. Hierdurch soll das Verwertungsverbot nach Art. 6 GDG zusätzlich organisatorisch gesichert werden. Die Zentralkartei hat nur die Aufgabe einer **Suchkartei**, mit deren Hilfe die am Gesundheitsamt über eine Person geführten Akten aufgefunden werden können. Hierzu sind nur formale, aber keine inhaltlichen Hinweise erforderlich.

Ich habe das Gesundheitsamt gebeten zu prüfen, ob die Möglichkeit einer weiteren Verschlüsselung besteht, mit deren Hilfe Rückschlüsse auf bestimmte Erkrankungen ausgeschlossen werden können. In Betracht kommen dabei auch organisatorische Maßnahmen.

Behindertenkartei

Bei der Prüfung wurde eine Behindertenkartei festgestellt, die offenbar nur zur Erstellung des Jahresgesundheitsberichts benötigt wird. Die Kartei enthält u. a. auch die **Diagnose** des Betroffenen. Diese spielt im Jahresgesundheitsbericht jedoch keine Rolle.

Da in der Kartei besonders sensible Daten enthalten sind, habe ich um Überprüfung gebeten, ob die Kartei in dieser Form (mit Diagnose?) geführt werden muß und ob sie nach Erstellung der Statistik gelöscht werden kann.

Anonyme AIDS-Beratung

Die anonyme AIDS-Beratungsstelle war räumlich und personell von den übrigen Sachgebieten des Gesundheitsamtes getrennt. In dem Journal, in dem die HIV-Tests dokumentiert werden, waren **keine Namen** von untersuchten Personen eingetragen. Zur Identifizierung der Testergebnisse dienen eine fortlaufende Journalnummer und ein vom Betroffenen angegebenes zusätzliches „Phantasiedatum". Das Testergebnis wird nur bei persönlicher Vorsprache — nicht am Telefon — mitgeteilt.
Ich habe diese Verfahrensweise ausdrücklich begrüßt.

Abrechnung von Nebentätigkeiten von Ärzten

Ärzte am Gesundheitsamt führen in amtlich anerkannter Nebentätigkeit Untersuchungen durch. Angaben zu den untersuchten Personen werden in ein **Leistungsbuch** eingetragen, das der Kontrolle über die Abführung eines Teils der Nebentätigkeitseinnahmen an den Dienstherrn dient.

Dieses Leistungsbuch ist nach einer Bekanntmachung des Staatsministeriums des Innern vom 21.12.1988 jedoch so zu führen, daß nicht der Name des Untersuchten, sondern eine laufende Nummer sowie der Auftraggeber und gegebenenfalls Datum und Aktenzeichen des Auftrags einzutragen sind. Dies dient der **Abschottung** dieses Untersuchungsbereichs gegenüber dem Amtsbereich, wie dies in Art. 6 GDG vorgeschrieben ist. Ich habe das Gesundheitsamt aufgefordert, künftig im Leistungsbuch die Namen der untersuchten Personen wegzulassen. Ferner habe ich um Prüfung gebeten, ob es für die Verwaltung ausreicht, wenn auf den Laufzetteln nur die im Leistungsbuch enthaltenen Angaben eingetragen sind.

2.3 Datenschutzkontrolle beim Bayer. Roten Kreuz

Erstmals habe ich beim Bayer. Roten Kreuz eine allgemeine Kontrolle durchgeführt. Beim **Präsidium** und bei einem **Kreisverband** wurden die Erhebung personenbezogener Daten, ihre Speicherung in automatisierten Dateien und manuell geführten Karteien sowie stichprobenweise die regelmäßigen Datenübermittlungen aus diesen Karteien und Dateien überprüft. Grobe Verstöße gegen datenschutzrechtliche Bestimmungen wurden nicht festgestellt.

Auf einem **Anmeldebogen des Präsidiums für Schwesterhelferinnen** wird nach detaillierten Angaben zum

Familienstand und zum Lebenslauf gefragt. Hier habe ich eine Begrenzung der Angaben auf dem Meldebogen auf den zur Durchführung des Lehrgangs erforderlichen Umfang gebeten. Die Mitgliederdatei Wasserwacht, die Dateien der Landesberatungsstelle für Aus- und Übersiedler, der Rettungsleitstelle in München und die Rückholdienstdatei waren noch nicht zum **Datenschutzregister** angemeldet. Im **Anmeldebogen** zum freiwilligen sozialen Jahr und in einem **Personalfragebogen** waren Fragen nach Konfession und Familienstand gestellt, ohne daß diese Fragen für die Aufnahme als Helferin im freiwilligen sozialen Jahr von Bedeutung sind. Ich habe um Änderung der Formulare gebeten.

Meldebögen für die Aufnahme in ein Müttergenesungsheim enthielten neben Fragen nach der Konfession auch detaillierte Fragen nach Familienstand und nach Akkord- oder Teilzeitarbeit der Mutter sowie nach Konfession und ehemaligem Beruf des Ehegatten der Mutter. Ich habe gebeten, bei diesen sensiblen Angaben im Fragebogen deutlich auf die Freiwilligkeit hinzuweisen.

Der geprüfte **Kreisverband** hatte zum Datenschutzregister zwei Dateien nachzumelden. Bei einer nicht mehr fortgeführten Datei mit personenbezogenen Daten habe ich die Löschung, bei zwei Karteien mit medizinischen Angaben über betreute Personen eine sichere Verwahrung gefordert.

2.4 Meldung von Patientendaten an Krebsregister (anonymisierte Führung von Krebsregistern)

Von einem Patienten bin ich darauf aufmerksam gemacht worden, daß den Patienten der Sinn und Zweck des von der Kassenärztlichen Vereinigung Bayern herausgegebenen **Nachsorgekalenders** und der damit verbundenen Übermittlung von Patientendaten an das **Nachsorgeregister** wohl nicht stets ausreichend erklärt werden. Möglicherweise besteht auch bei den Klinikärzten, die am Ende der stationären Behandlung dem Patienten einen Nachsorgekalender aushändigen, manchmal Unsicherheit über die rechtlichen Grundlagen der mit dem Nachsorgekalender verbundenen **Tumordokumentation**. Aus der Sicht des Datenschutzes, den der Patient zu Recht einfordert, stellt sich die Zusammenarbeit zwischen den Kliniken, Tumorregistern, niedergelassenen Ärzten und der zentralen Dokumentation der Kassenärztlichen Vereinigung Bayerns folgendermaßen dar:

- Speichert eine Klinik im Rahmen des Behandlungsverhältnisses ihre Patienten in den eigenen **Klinikdateien**, so ist dies durch Art. 26 Abs. 2 des Bayer. Krankenhausgesetzes erlaubt. Die Einwilligung des Patienten hierzu ist also nicht erforderlich.

- Soweit Kliniken ihre patientenbezogene Dokumentation im Wege der **„Datenverarbeitung im Auftrag"** in einer anderen Klinik oder in den Tumorregistern München, Erlangen oder Würzburg speichern lassen, ist dies durch Art. 26 Abs. 4 und 5 des Bayer. Krankenhausgesetzes gestattet; eine vorausgehende Aufklärung oder Einwilligung des Patienten ist nicht erforderlich. Voraussetzung ist, daß die erforderlichen Datensicherungsmaßnahmen getroffen werden. Auch im Falle der Auftragsdatenverarbeitung gehören die Patientendaten den auftraggebenden (angeschlossenen) Kliniken. Nur sie haben für die Daten mit identifizierenden Merkmalen eine Abrufberechtigung.

  Für wissenschaftliche Auswertungen durch das **Tumorregister** stehen nur die **anonymen medizinischen Daten ohne identifizierende Merkmale** zur Verfügung.

- Der **Nachsorgekalender** wird dem Patienten nach der Behandlung in der Regel in der Klinik ausgehändigt. Er spielt in diesem Zusammenhang folgende Rolle: Wenn der Patient die auf Seite 5 des Nachsorgekalenders vorgesehene Einverständniserklärung unterschrieben hat, kann jeder Arzt, dem der Patient den Kalender vorlegt, über die Kalendernummer zum einen etwaige bei der Dokumentation der Kassenärztlichen Vereinigung Bayern (KVB) anonym gespeicherte Daten abrufen und zum anderen seine eigenen Erkenntnisse über den Patienten der Dokumentation hinzufügen. Auf diesem Weg kann beispielsweise eine Klinik zu den von ihr selbst abgespeicherten Behandlungsdaten ihrer stationären Patienten zusätzlich die Daten der KVB-Nachsorgedokumentation über ambulante Behandlungen nutzen. Der für die abrufende Stelle personenbezogene Datenabruf bei der KVB ist durch Einwilligung im Nachsorgekalender und dessen Vorlage bei der abrufenden Stelle gedeckt.

  Die **anonyme Speicherung** von Patientendaten bei der KVB entsteht dadurch, daß der behandelnde Arzt auf einem von der KVB herausgegebenen Erfassungsbogen Patientendaten **ohne identifizierende Angaben** unter der Nachsorgekalendernummer an die KVB schickt. Für diese anonyme Datenübermittlung ist keine Einwilligung des Patienten erforderlich. Gleichwohl erhält der Patient durch die Einwilligungserklärung auf dem Nachsorgekalender sowohl eine Information als auch ein Mitwirkungsrecht.

  Ich habe das Tumorregister, aus dessen Bereich die Eingabe stammte, gebeten, die Ärzte in den angeschlossenen Kliniken entsprechend zu informieren, damit sie ihrerseits die Patienten über das Verfahren des Nachsorgekalenders ausreichend unterrichten können. Entsprechende Hinweise empfehlen sich bei anderen Tumorregistern.

2.5 Anonymer unverknüpfbarer HIV-Test (AUT)

Wie im 12. Tätigkeitsbericht dargestellt, habe ich einen von der Gesellschaft für Strahlen- und Umweltforschung (GSF) erstellten Studienplan für einen anonymen unverknüpfbaren HIV-Test (AUT) daraufhin überprüft, ob nach dem vorgesehenen Verfahren die vom Innenministerium geforderte **irreversible Anonymisierung der Blutproben** und die Unverknüpfbarkeit des Testergebnisses mit bestimmten Patienten sichergestellt sind. Gegen das vorgelegte Konzept hatten sich keine Bedenken ergeben. Seit Mitte 1991 beteiligen sich nun fünf Kliniken an einer Machbarkeitsstudie für den AUT.

Im Berichtsjahr habe ich das Erhebungsverfahren und die **organisatorisch-technische Ausgestaltung des Anonymisierungsverfahrens** in vier Labors der öffentlich-rechtlichen Kliniken überprüft.

Das **Erhebungsverfahren** sieht folgende Sicherungsmaßnahmen vor: Von einer Blutprobe werden in der Klinik nur diejenigen Daten erfaßt, die für die Auswertung beim MEDIS-Institut der GSF erforderlich sind. Diese Daten geben dem Institut keine Möglichkeit zum Rückschluß auf bestimmte Patienten. Bei den Auswertungsdaten handelt es sich um Altersklasse, Geschlecht, Klinikbereich sowie ambulant/stationär. Diese Daten werden, zusammen mit einer laufenden Nummer, die das Kliniklabor speziell für diesen Zweck vergibt, noch in der Klinik derart verschlüsselt, daß ein Rückgriff auf diese Daten und ihre Zuordnung zu bestimmten Patienten in der Klinik nicht mehr möglich ist. Die Auswahl, Codierung und Speicherung der Blutproben erfolgt in der Klinik stets auf einem unvernetzten Personal Computer. Auf diesem Rechner wird, um Doppelerfassungen zu vermeiden, lediglich eine über einen bestimmten Algorithmus **irreversibel verschlüsselte Datei aller Probenspender** gespeichert. Die Patientendatei, die zur Auswahl und Codierung der Probendatei notwendig ist, wird nach dem Erhebungsverfahren (Erstellen des Probencodes) im PC gelöscht. Die das Kliniklabor verlassenden Daten mit den Probencodes sind irreversibel anonymisiert.

Die Blutproben, die das Kliniklabor verlassen, sind durch den anonymen Probencode (Barcode) gekennzeichnet. Im Labor der GSF werden die Blutproben analysiert. Die Untersuchung der Blutproben läuft maschinell ab. Die Ergebnisse werden in einer Ergebnisdatei maschinell aufgezeichnet. Auch wenn die **Laborkraft** feststellt, daß eine Probe HIV-positiv ist, ist es ihr nicht möglich, herauszubekommen, von welcher Klinik welche Probe kommt, weil für sie der Probencode nicht interpretierbar ist.

Beim ersten Auswertungslauf der Ergebnisdatei im MEDIS-Institut der GSF konnte ich mich davon überzeugen, daß eine **Zuordnung** der Ergebnisse zu einer bestimmten Probe nicht möglich ist. In den einzelnen Klassen (Altersklasse, Geschlecht, Klinikbereich, ambulant/stationär) werden nur dann Zahlen ausgewiesen, wenn die vorgegebenen Mehrlingsbedingungen gegeben sind, d.h. mindestens 6 Fälle und davon höchstens 4 mit HIV-positiv.

Nach jedem **Auswertungslauf** der Ergebnisdatei, der aus verfahrenstechnischen Gründen alle zwei Wochen und auf einem isolierten Personal Computer abläuft, wird ein Protokoll erstellt, aus dem ersichtlich ist, wer anwesend war. Die Vier-Augen-Kontrolle ist gewährleistet, da mindestens zwei Personen, nämlich eine Laborkraft, welche die Ergebnisdatei mitbringt, und ein Mitarbeiter des MEDIS-Instituts, der das Programm startet, für den Programmablauf von Nöten sind. Nach dem Auswertungslauf werden alle temporären Dateien gelöscht und nur die anonymisierte Auswertungsdatei bleibt im PC des MEDIS-Instituts gespeichert. Die anonymisierte Auswertungsdatei enthält klassenbezogen (Altersklasse, Geschlecht, Klinikbereich, ambulant/stationär) die Zahl der HIV-negativen und -positiven Proben unter Beachtung der oben beschriebenen Mehrlingsbedingungen. Der Inhalt der Diskette mit der Ergebnisdatei ist für das Labor selbst nicht auswertbar, da die Programme zur Interpretation der Ergebnisdatei im Labor nicht verfügbar sind. Die Studie soll am 31.12.1991 abgeschlossen sein. Der AUT liefert den teilnehmenden Kliniken zuverlässigere Angaben über Anzahl und Verteilung der HIV-positiven Personen unter ihren Patienten. Diese Angaben ermöglichen eine genauere Bedarfsplanung und gezielte Präventionsmaßnahmen in den Kliniken.

Der Datenschutz und die Datensicherheit sind in jedem einzelnen Arbeitsschritt gewährleistet.

2.6 Automatisierte Krankendokumentation mit dem Verfahren KLIMACS

Im Auftrag des Bundesministers für Gesundheit hat die Paul-Ehrlich-Gesellschaft (PEG) für Kliniken ein Krankendokumentationssystem „KLIMACS" auf PC-Basis entwickelt. Mit KLIMACS soll die Krankengeschichte von AIDS-Patienten und HIV-Infizierten unter Beachtung des Datenschutzes als **Teil der Krankenakte** erfaßt werden. Ambulante und stationäre Versorgungsleistungen sollen unterstützt werden. Eine **anonyme statistische Auswertung** ist vorgesehen.

Für dieses ADV-Verfahren hat die PEG „Datenschutzanforderungen an KLIMACS und seine Anwender" aufgestellt. Nach Auffassung des Bundesbeauftragten für den Datenschutz entsprechen diese seinen Anforderungen an eine **sichere Datenverarbeitung** mit dem Programm KLIMACS. Die Details des Einsatzes des Programms in den einzelnen Kliniken müssen jeweils vor Ort festgelegt und vom zuständigen Landesbeauftragten für den Datenschutz überprüft werden.

Der Bundesdatenschutzbeauftragte hat einige Kliniken benannt, die an einer Anwendung des Programms interessiert sind. Diese Kliniken habe ich über die Bewertung von KLIMACS durch den Bundesdatenschutzbeauftragten unterrichtet und um nähere Angaben zur Installation des Programms in der Klinik gebeten, damit ich die erforderliche Prüfung vor Ort durchführen kann. Dabei habe ich um Mitteilung des **Datensatzes** gebeten, der in der Klinik tatsächlich genutzt werden soll. Ich habe ferner um Mitteilung gebeten, ob mit KLIMACS nur zur **Behandlung** erforderliche Daten oder auch Daten **nur für Forschungszwecke** erhoben und in dem System gespeichert werden sollen. Desweiteren habe ich nach den in der Klinik beabsichtigten **Datensicherungsmaßnahmen** und nach eventueller Verbindung des DV-Systems KLIMACS mit anderen Arbeitsbereichen des Krankenhauses gefragt, um die Risiken des DV-Einsatzes bewerten zu können.

Meine Fragen konnten bisher von keiner angeschriebenen Klinik beantwortet werden. Die meisten machten geltend, daß eine Beantwortung erst nach einer Probeinstallation von KLIMACS möglich sei.

Eine Klinik hat das KLIMACS-Programm inzwischen erhalten. Die Anwendung wird von mir rechtlich und organisatorisch überprüft werden.

2.7 Fernwartung eines Klinik-DV-Systems

Die Krankenhäuser entwickeln ihre DV-Verfahren nur zum Teil in Eigenregie. Komplexere Verfahren werden von Software-Herstellerfirmen im Auftrag und in Zusammenarbeit mit einer Klinik entwickelt und anschließend auch anderen Kliniken angeboten.

Soweit die Wartung von DV-Verfahren in Krankenhäusern vorgenommen wird, gibt es hinsichtlich der Datensicherheit und des Datenschutzes in der Regel keine rechtlichen Probleme, da sie unter Aufsicht der berechtigten Mitarbeiter des Krankenhauses durchgeführt wird. Grundsätzlich dürfen **keine Patientendaten im Rahmen der Wartung die Klinik verlassen.**

Datenschutzfragen ergeben sich aber, wenn die Klinik aus **Kostengründen** von der Wartung vor Ort auf Fernwartung z.B. vom Ort der Software-Herstellerfirma aus umsteigen will. Fernwartung hätte zur Folge, daß Systemspezialisten der Firma über die Postleitung von der Firma aus auch auf den einzelnen Patienten identifizierende Merkmale im DV-Verfahren zugreifen können. Die im Krankenhaus besonders geschützten Patientendaten könnten auf diesem Weg **aus dem Schutzbereich des Krankenhauses heraus** in die Hände von Personen gelangen, für die weder die ärztliche Schweigepflicht noch ein Zeugnisverweigerungsrecht gilt.

Der mögliche Zugriff auf identifizierende Merkmale der Patienten wirft somit die Frage auf, ob die Klinik zur Offenbarung solcher Daten im Sinne von § 203 Abs. 2 StGB befugt ist. Ich habe daher bei einem Krankenhaus-DV-Projekt, bei dem Fernwartung erwogen wird, den Träger der Klinik aufgefordert, nach Möglichkeiten zu suchen, um dieses Problem zu lösen. Hier muß rechtzeitig, schon bei der Konzeption des Verfahrens, für den gebotenen Schutz der Patientendaten gesorgt werden.

Ferner ist beabsichtigt, auf technisch-organisatorischem Gebiet Möglichkeiten zu überprüfen, um **die mit Fernwartungsfragen verbundenen Risiken** zu reduzieren. Mit den Staatsministerien für Arbeit, Familie und Sozialordnung (Krankenhausrecht), des Innern (Arztrecht) und der Justiz (ärztliche Schweigepflicht) werde ich die rechtlichen Gestaltungsmöglichkeiten erörtern. Dabei wird auch die Entscheidung des Bundesgerichtshofs vom 10.7.1991 zur Einschaltung einer gewerblichen Verrechnungsstelle zu berücksichtigen sein (s. auch Nr. 2.1). Der BGH führt dort in der Begründung u.a. aus, daß wirtschaftliche Erwägungen die Verletzung der ärztlichen Schweigepflicht nicht zu rechtfertigen vermögen. Auch zur Fernwartung werden vor allem wirtschaftliche Erwägungen ins Feld geführt. Das Urteil betrifft daher eine ähnliche Situation.

3. Sozialbehörden

3.1 Bürgereingaben

Im Berichtsjahr wandten sich wiederum Bürger mit den unterschiedlichsten Beschwerden wegen Verletzungen des **Sozialgeheimnisses** an mich.

Ein Petent wies darauf hin, daß ein Landratsamt auf dem **Überweisungsträger** für eine Zahlung an einen Sozialleistungsträger in der Zeile „Verwendungszweck" die Angabe „Abtreibung, ... (Name)" vermerkt hatte. Ich habe deutlich gemacht, daß dies zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch nicht erforderlich und deshalb nach § 35 SGB I unzulässig war. Das Amt hat versichert, daß es sich um einen Einzelfall gehandelt habe; derartige Verwendungszwecke würden sonst nicht auf Überweisungsträgern vermerkt werden. Ich habe das Amt aufgefordert, meine Rechtsauffassung allen mit solchen Vorgängen befaßten Bediensteten gegen Unterschrift zur Kenntnis zu geben.

3.2 Besetzung der Gremien von Betriebskrankenkassen

Bereits im 12. Tätigkeitsbericht habe ich auf das **Abschottungsgebot** gem. § 63 Abs. 3a SGB IV bei Betriebskrankenkassen hingewiesen. Bei der Prüfung einer Betriebskrankenkasse im Berichtsjahr habe ich feststellen müssen, daß ein **Stadtdirektor als Mitglied der Widerspruchsstelle** benannt war. Des weiteren wurden mehrere leitende Angestellte mit Personalverantwortung als Arbeitgebervertreter in den Vor-

stand und die Vertreterversammlung der Betriebskrankenkasse entsandt. In Übereinstimmung mit dem Staatsministerium für Arbeit, Familie und Sozialordnung vertrete ich zur Besetzung dieser Gremien folgende Auffassung:

1. **Auf Widerspruchsstellen** findet die Vorschrift des § 63 Abs. 3 a SGB IV Anwendung. Ausgeschlossen von der Beratung und Abstimmung in der Widerspruchsstelle sind nach dieser Vorschrift Angehörige der Personalverwaltung des Betriebes, dem der Arbeitnehmer angehört, über dessen Widerspruch entschieden werden soll. Dabei kommt es nicht auf die Größe der Personalverwaltung und die Position des Mitglieds der Widerspruchsstelle an. Sobald jemandem in seiner beruflichen Tätigkeit die Personalverwaltung des Errichtungsbetriebes unterstellt ist, ist er ein Angehöriger der Personalverwaltung. Daher darf er an der Sitzung nicht teilnehmen, sobald in dieser personenbezogene Daten erörtert werden sollen. Dieses Verbot betrifft auch den von der Betriebskrankenkasse in die Widerspruchsstelle entsandten Stadtdirektor, wenn diesem die Personalverwaltung unterstellt ist.

   Zur Sicherstellung des Abschottungsgebotes bieten sich zwei Möglichkeiten an. Entweder es wird vor jeder Sitzung geprüft, ob und ggf. bei welchen Tagesordnungspunkten das Mitglied von der Teilnahme ausgeschlossen ist, oder die Widerspruchsstelle wird umbesetzt.

2. Das Abschottungsgebot ist auch von den Mitgliedern der **Vertreterversammlung** bzw. den Mitgliedern des **Vorstandes** zu beachten. Nachdem auch leitende Angestellte mit Personalverantwortung als Arbeitgebervertreter in diese Gremien entsandt wurden, ist vor jeder Sitzung, in der ausnahmsweise personenbezogene Daten i.S. des § 63 Abs. 3 a Satz 3 SGB IV zur Sprache kommen sollen, zu prüfen, ob das Mitglied von der Teilnahme ausgeschlossen ist.

Ich habe die Betriebskrankenkasse über diese Rechtsauffassung in Kenntnis gesetzt. Eine Antwort der Betriebskrankenkasse steht noch aus.

3.3 Hinweis der Krankenkasse an Arbeitgeber bei Schadensersatzanspruch

Im 12. Tätigkeitsbericht habe ich mich zur Praxis verschiedener Krankenkassen geäußert, die den Arbeitgeber auf das Vorliegen eines Drittverschuldens hinweisen, wenn ein Arbeitnehmer einen Körperschaden erlitten hat. Wegen fehlender originärer Aufgaben der Krankenkasse und fehlender Zustimmung der Arbeitnehmer halte ich diesen Hinweis für unzulässig.

Die Landesverbände der Krankenkassen haben sich dieser Auffassung angeschlossen. Für die Offenbarung des Drittschädigers gebe es weder eine rechtliche Grundlage noch sei eine konkludente Einwilligung des Arbeitnehmers anzunehmen. Andererseits sei aber auch das berechtigte Interesse des Arbeitgebers, sich bei Drittverschulden schadlos zu halten, zu berücksichtigen. Um den unterschiedlichen Interessen gerecht zu werden, wurde vorgeschlagen, im Unfallfragebogen die Möglichkeit vorzusehen, daß der Arbeitnehmer der Mitteilung eines eventuellen Mitverschuldens an seinen Arbeitgeber zustimmt. Falls der Arbeitnehmer der Weitergabe nicht zustimmt, hat er ein entsprechendes Feld anzukreuzen.

Rechtlich unbedenklich wäre eine Einwilligungserklärung, die formal im räumlichen Zusammenhang mit der Unterschrift steht und drucktechnisch hervorgehoben ist. Es sollte die Verweigerung der Einwilligung angenommen werden, wenn die betreffende Zeile des Fragebogens übersehen wird. Außerdem sollte in allgemein verständlichen Worten zum Ausdruck gebracht werden, daß die Erteilung der Einwilligung freiwillig ist und die Verweigerung sich nicht auf die Leistungen der Krankenkasse auswirkt.

Ich habe den Landesverbänden der Krankenkasse diese Rechtsauffassung mitgeteilt. Ein mit mir abgestimmter Text ist den Mitgliedskassen mitgeteilt worden.

3.4 Datenübermittlung von Krankenkassen an die Sozialhilfeverwaltung

In einer Eingabe wurde ich um Prüfung gebeten, ob Krankenkassen **ohne Auftrag** regelmäßig Daten über **Krankenhausaufenthalte** ihrer Mitglieder an ein Landratsamt — Sozialhilfeverwaltung — übermitteln dürfen. Die Befürchtung einer unzulässigen Datenübermittlung bestätigte sich jedoch nicht. Die Überprüfung ergab vielmehr, daß das Landratsamt — Sozialhilfeverwaltung — die Krankenkassen in Fällen von laufender Sozialhilfe in Form von Hilfe zum Lebensunterhalt oder Hilfe zur Pflege mittels eines Formblattes ersucht, im Falle einer Krankenhausbehandlung des Hilfeempfängers den Aufnahme- und Entlassungstag mitzuteilen.

In Übereinstimmung mit dem Staatsministerium für Arbeit, Familie und Sozialordnung habe ich gegen die **Offenbarung des Aufnahme- und Entlassungstages** bei einem stationären Krankenhausaufenthalt keine datenschutzrechtlichen Bedenken geäußert. Bei der Beurteilung der Frage ist darauf abzustellen, ob die Offenbarung gem. § 69 SGB X zur Erfüllung einer gesetzlichen Aufgabe der Sozialhilfeverwaltung erforderlich ist. Die Erforderlichkeit hat sich im vorliegenden Falle aus der Tatsache ergeben, daß die Sozialhilfeverwaltung mangels zuverlässiger Meldung durch die Betroffenen keine Kenntnis vom Krankenhausaufenthalt erhält und deshalb nicht sicherstellen

kann, daß Hilfeempfänger bei einem Krankenhausaufenthalt keine unberechtigten Sozialhilfeleistungen erhalten.

Der Übermittlung steht auch nicht entgegen, daß im Sozialhilfebescheid darauf hingewiesen wird, daß die Aufnahme in ein Krankenhaus unverzüglich und unaufgefordert der Sozialhilfeverwaltung angezeigt werden muß. Nach Auskunft der Sozialhilfeverwaltung werden nämlich allenfalls 15 % der Krankenhausaufenthalte von den Hilfeempfängern tatsächlich angezeigt. Da die Sozialhilfeverwaltung demnach in 85 % der Fälle den Krankenhausaufenthalt nicht erfährt, wäre sie auf ständige Nachfragen bei (auch gesunden) Sozialhilfempfängern angewiesen. Demgegenüber werden berechtigte Interessen der Sozialhilfeempfänger durch die Mitteilung der Krankenkasse nicht unangemessen beeinträchtigt.

3.5 Weiterleitung von Kindererziehungsleistungen an Heimbewohnerinnen durch die Sozialämter

Nach Inkrafttreten des Kindererziehungsleistungsgesetzes mußte zum 01. Oktober 1987 die Auszahlung der Geldleistungen an Mütter der Geburtsjahrgänge vor 1906 organisiert werden. Dabei tauchte das Problem auf, daß eine unmittelbare Auszahlung des Geldes an Heimbewohnerinnen meist nicht möglich war, weil die Deutsche Bundespost nicht über die aktuellen Anschriften der Rentenempfängerinnen verfügte. Daher wurde in den Fällen, in denen bei Heimbewohnerinnen der Träger den Sozialhilfeersatz geltend machen konnte, die Leistung für Kindererziehung zusammen mit der Rente an den Sozialhilfeträger überwiesen. Dieser hatte die Leistung an die Mutter weiterzuleiten. Dieses Verfahren wurde beibehalten, da die Mütter im allgemeinen nicht über ein eigenes Konto verfügten und nicht gezwungen werden sollten, lediglich wegen der Leistung für Kindererziehung ein eigenes Konto zu eröffnen und mit den laufenden Gebühren belastet zu werden.

Der Bundesbeauftragte für den Datenschutz hält das derzeitige Verfahren für datenschutzrechtlich bedenklich. Es sei deshalb notwendig, daß vor der Weiterleitung solcher Leistungen an ein Heim Heimbewohnerinnen befragt werden, ob sie die Erziehungsgeldleistung auf ein eigenes Konto oder über die Heimleitung bar ausbezahlt haben möchten.

Das Bayerische Staatsministerium für Arbeit, Familie und Sozialordnung sowie die Bayerischen Kommunalen Spitzenverbände halten eine derartige Befragung nicht für sinnvoll. Die Tatsache, daß die Heimbewohnerin Sozialhilfe beziehe, sei dem Heim bereits bekannt, da die Abrechnung der Heimkosten mit dem Sozialhilfeträger direkt erfolge. Insoweit könnten aus der Weiterleitung der Kindererziehungsleistungen **keine neuen Erkenntnisse** gewonnen werden. Im übrigen erscheine im Hinblick auf die hohe Betreuungsbedürftigkeit der meisten Heimbewohnerinnen (bereits ein Drittel von ihnen befinde sich in der Pflegeabteilung) sowie das hohe Durchschnittsalter (ca. 86 Jahre) eine derartige Befragung der Heimbewohnerinnen weder sinnvoll noch wegen des unzumutbaren Verwaltungsaufwands vertretbar.

Die Auffassung des Staatsministeriums für Arbeit, Familie und Sozialordnung teile ich. Eine Änderung des bisherigen Auszahlungsverfahrens halte ich daher nicht für erforderlich.

3.6 Krankenkassenzugehörigkeit der Mitgliedsbetriebe einer Handwerksinnung

Eine Handwerksinnung bat mich um Überprüfung folgenden Sachverhalts:

Seit 1.1.1990 sei für alle ihre Mitgliedsbetriebe die **Zuständigkeit einer Innungskrankenkasse** gegeben. Trotzdem habe eine AOK einem Innungsbetrieb, der seine Arbeitnehmer zur Innungskrankenkasse umgemeldet hatte, einen **Fragebogen** mit Angaben zur Prüfung der Krankenkassenzugehörigkeit zur Beantwortung übersandt. Nach Ansicht der Innung sei die AOK nicht mehr berechtigt gewesen, derartige Daten nach dem Übergang der Versicherten an die Innungskrankenkasse zu erheben. Außerdem gehe der Fragebogen weit über die zur Prüfung der Kassenzuständigkeit erforderlichen Daten hinaus; er bedeute vielmehr eine umfassende **Ausforschung** der gesamten Betriebsstruktur.

Das Staatsministerium für Arbeit, Familie und Sozialordnung sieht für derartige Auskünfte, die der Feststellung der Kassenzugehörigkeit dienen sollten, in § 98 Abs. 1 Satz 2 und § 21 SGB X eine ausreichende Rechtsgrundlage. Im Vordergrund stehe dabei die fachliche Frage, welche Kriterien zur Abgrenzung der Kassenzugehörigkeit in Frage kämen. Der Fragebogen gebe aufgrund der vielfältigen Rechtsprechung zur Abgrenzung der Kassenzugehörigkeit durchaus verwertbare Hinweise für diese Abgrenzung. Die Berechtigung der AOK, nach §§ 98 Abs. 1 Satz 2 und 21 SGB X an einzelne Arbeitgeber unmittelbar heranzutreten, um die Frage der **Kassenzugehörigkeit zu klären**, ist durch den Anschluß der ganzen Innung an die Innungskrankenkasse nicht ausgeschlossen worden. Es kommt auch nach diesem Anschluß für die Kassenzugehörigkeit jedes einzelnen Innungsbetriebes darauf an, ob er die Voraussetzungen für die Zugehörigkeit zu den jeweiligen Kassen aufweist. Verhandlungen auf Verbandsebene dürften diese Einzelfallprüfungen kaum ersetzen können.

Die Auffassung des Staatsministeriums für Arbeit, Familie und Sozialordnung teile ich. Da mir keine gegenteiligen fachlichen Erkenntnisse vorliegen, sehe ich keinen Anlaß, die Übersendung des Fragebogens an den Innungsbetrieb und die einzelnen Fragen zur Abgrenzung der Kassenzugehörigkeit zu beanstanden.

4. Polizei

4.1 Zur Lage des Datenschutzes

Nach Inkrafttreten des Dritten Gesetzes zur Änderung des Polizeiaufgabengesetzes (PAG) am 1. Oktober 1990 gilt es, die **Richtlinien** und **Dienstanweisungen** für die polizeiliche Datenverarbeitung den neuen gesetzlichen Bestimmungen **anzupassen**. Die Errichtungsanordnungen für bestehende Dateien, in denen Inhalt, Zweck, Speicherungsdauer, Nutzung, Zugriff u.a. im einzelnen näher geregelt sind, sind zu überarbeiten. Die Errichtungsanordnung für den kriminalpolizeilichen Aktennachweis (KAN) muß darauf überprüft werden, ob unter dem Gesichtspunkt der Erforderlichkeit auf weitere Speicherungen verzichtet und für bestimmte Delikte von geringerer Bedeutung kürzere Speicherungsfristen vorgesehen werden sollen. In einer **Dienstanweisung KAN** hat das Innenministerium die Erfahrungen der letzten Jahre bei der Anwendung dieser Datei zusammengefaßt. Diese Dienstanweisung dürfte nicht nur zur einheitlichen Handhabung der Datei beitragen, sondern auch Anwendungsprobleme beheben, zumindest erheblich verringern.

Die Polizei erhält nunmehr in den meisten Fällen, in denen sie personenbezogene Daten speichert, Kenntnis vom **Ausgang des Justizverfahrens.** Bei Einstellung des Verfahrens nach § 170 Abs. 2 StPO fehlt ihr aber regelmäßig die für die Beurteilung der weiteren Datenspeicherung notwendige Kenntnis, ob nach Auffassung der Justiz der Tatverdacht entfallen ist. Eine Einigung über entsprechende Mitteilungen der Staatsanwaltschaft konnte noch nicht erzielt werden.

Die Errichtungsanordnung für die **Datei Vorgangsverwaltung** ist in Überarbeitung. Sie soll auf die polizeilichen Zwecke Sachbearbeitung und Verbrechensbekämpfung ausgeweitet werden. Hierzu habe ich eine Reihe von Verbesserungen des Datenschutzes gefordert.

Die **Ausrüstung** der Polizei mit Arbeitsplatzcomputern (APC) wurde fortgeführt. Die technische Ausstattung der Dienststellen mit DV-Geräten wird voraussichtlich Anfang 1992 abgeschlossen sein. Die Zahl der zum Datenschutzregister gemeldeten APC-Anwendungen hat im Berichtszeitraum weiter zugenommen. Auf die Entwicklung und Kontrolle der Anwendungen werde ich in den nächsten Jahren mein besonderes Augenmerk richten. Mit entsprechenden Prüfungen habe ich im Berichtszeitraum begonnen.

Während der Landesgesetzgeber mit dem neuen Polizeiaufgabengesetz eine ausreichende gesetzliche Grundlage für die Tätigkeit der Polizei auf dem Gebiet der Gefahrenabwehr einschließlich der Gefahrenvorsorge und der Vorhaltung von Informationen für künftige Ermittlungen geschaffen hat, fehlt es noch immer an **normenklaren bundesrechtlichen Regelungen** der polizeilichen Datenerhebung und -verarbeitung **zur Strafverfolgung.** Es ist zu hoffen, daß das Gesetz zur Bekämpfung der Rauschgiftkriminalität und anderer Formen der organisierten Kriminalität (OrgKG) vom Bundestag alsbald verabschiedet wird, damit endlich Klarheit darüber geschaffen wird, was die Polizei bei der Verfolgung von Straftaten darf und was sie nicht darf.

Breiten Raum in der öffentlichen Diskussion nahm wieder das **Verhältnis von Datenschutz und polizeiliche Aufgabenerfüllung** ein. Für die fehlenden Fahndungserfolge im Bereich der Terrorismusbekämpfung wurden teilweise auch Behinderungen der polizeilichen Informationssammlung und -auswertung durch datenschutzrechtliche Bestimmungen in Gesetzen und Richtlinien verantwortlich gemacht. Ich habe mich in diesem Zusammenhang für eine **unvoreingenommene Bestandsaufnahme** und Überprüfung angeblicher Behinderungen der Polizei durch den Datenschutz ausgesprochen. In erster Linie sollte hier die Polizei diejenigen Bestimmungen, Richtlinien und sonstigen Hindernisse benennen, durch die sich die Polizei an einer effektiven Arbeit gehindert sieht. Dann kann geklärt werden, welche Beschränkungen angesichts der offenkundigen Erfolglosigkeit der Polizei wegfallen sollen. Das Verhältnis Datenschutz — polizeiliche Arbeit ist keine Einbahnstraße. Eine Rücknahme von als überzogen erkannten Bestimmungen muß möglich sein.

Während auf der einen Seite eine Revision datenschutzrechtlicher Beschränkungen polizeilicher Arbeit für notwendig gehalten wird, wurden auf der anderen Seite weitere Verschärfungen des Datenschutzes gefordert:

- Die Mehrheit der Datenschutzbeauftragten lehnte den Entwurf des Bundesrats zur Bekämpfung der organisierten Kriminalität wegen zu tiefer Eingriffe in das informationelle Selbstbestimmungsrecht ab.

- Unter den Datenschutzbeauftragten wurde die Forderung nach Einstellung des Betriebs der Staatsschutzdatei APIS, die Ansatzpunkte für polizeiliche Fahndung liefern soll, diskutiert. In zahlreichen Bundesländern wird APIS nur noch mit erheblichen Einschränkungen betrieben.

4.2 Schwerpunkte

Schwerpunkte meiner Tätigkeit im Polizeibereich waren

- allgemeine Kontrollen von Dateien und Karteien,
- die Prüfung polizeilicher Errichtungsanordnungen für bereits bestehende Dateien auf der Grundlage des novellierten Polizeiaufgabengesetzes,

- die Prüfung geplanter oder geänderter Datenverarbeitungsverfahren,
- Bürgereingaben.

Meine Geschäftsstelle wurde bei der Entwicklung neuer DV-Vorhaben beteiligt. Bei wichtigen Vorhaben werde ich schon vor dem Erlaß der Errichtungsanordnung, die für den erstmaligen Einsatz eines automatisierten Verfahrens gemäß Art. 47 PAG vorgeschrieben ist, informiert. Datenschutzrechtliche Gesichtspunkte können dadurch bereits in der Planungsphase eines Verfahrens eingebracht und berücksichtigt werden. So habe ich mich auch bereits zu den Vorarbeiten für eine Datei „Gewalttäter Sport" sowie zur Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung — Verbrechensbekämpfung (PSV)" äußern können.

4.3 Erfahrungen mit dem neuen Polizeiaufgabengesetz (PAG)

Nennenswerte Schwierigkeiten bei der Anwendung der neuen Vorschriften über die polizeiliche Datenerhebung und -verarbeitung sind im Berichtszeitraum nicht bekannt geworden.

Kontrolle besonderer Mittel der Datenerhebung

Die besonderen Mittel der polizeilichen Datenerhebung (längerfristige Observation, verdeckter Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und -aufzeichnungen sowie zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Worts, Einsatz verdeckter Ermittler) greifen besonders tief in das informationelle Selbstbestimmungsrecht ein. Deshalb ist mir die effektive Kontrolle dieser Einsätze ein besonders wichtiges Anliegen.

Meine im Gesetzgebungsverfahren geäußerte Befürchtung, eine wirksame Datenschutzkontrolle des Einsatzes besonderer Erhebungsmittel sei ohne gesetzliche Verankerung einer Aufzeichnungspflicht nicht gewährleistet, hat sich nicht bestätigt. Das Innenministerium hat vielmehr in der Vollzugsbekanntmachung zum PAG festgelegt, daß der Einsatz besonderer Mittel gesondert aufzuzeichnen ist und die Aufzeichnung auch zur Datenschutzkontrolle herangezogen werden kann. Eine inzwischen durchgeführte Prüfung bei einem Polizeipräsidium hat die volle Nachprüfbarkeit des Einsatzes besonderer Mittel ergeben. Da die Polizei zum Zwecke der Koordinierung im eigenen Interesse eine weitgehend zentrale Dokumentation der Einsätze vornimmt, können die jeweils speichernden Stellen bei Datenschutzkontrollen die Einsätze in ihrem Bereich nachweisen (vgl. Nr. 4.5.1).

Auskunft über Datenempfänger

Nach dem Wortlaut des Art. 48 Abs. 1 PAG erteilt die Polizei dem Betroffenen auf Antrag Auskunft über die zu seiner Person gespeicherten Daten.

Nach der vom Bayer. Verwaltungsgerichtshof im Beschluß vom 31.3.1991 vertretenen Auffassung erstreckt sich der Auskunftsanspruch auch auf die Stellen, denen erkennungsdienstliche Unterlagen übermittelt wurden. Der Verwaltungsgerichtshof begründet dies damit, Art. 48 Abs. 1 Satz 1 PAG lasse sich nicht dahingehend auslegen, daß er auch die Auskunft über Empfängerstellen umfasse. Es bestehe deshalb eine „Regelungslücke", die durch eine analoge Anwendung von Art. 48 PAG zu schließen sei. Diese Entscheidung ist aus datenschutzrechtlicher Sicht zu begrüßen. Nach der Entstehungsgeschichte und der Absicht des Gesetzgebers ist allerdings eher anzunehmen, daß dem Betroffenen, der nach dem Regierungsentwurf gar keinen Auskunftsanspruch erhalten sollte, im Spannungsverhältnis zwischen informationellem Selbstbestimmungsrecht und öffentlicher Sicherheit nur ein Anspruch auf die über ihn gespeicherte Daten, **nicht aber über Herkunft und Empfänger** der Daten eingeräumt werden sollte. Mit Rücksicht auf den Schutz der öffentlichen Sicherheit sollte der Betroffene nur die notwendigen Ansprüche erhalten. Das Bundesverfassungsschutzgesetz hat in § 13 Abs. 3 die Verpflichtung zur Auskunft über die Herkunft der Daten und die Empfänger von Übermittlungen ausdrücklich ausgeschlossen.

Im Ergebnis hat es der Bayer. Verwaltungsgerichtshof im zu entscheidenden Fall jedoch für gerechtfertigt angesehen, die vom Kläger begehrte Auskunft zu verweigern. Denn die mit der Bekanntgabe der Empfängerstellen verbundene Offenbarung der polizeilichen Meldewege sei mit dem Geheimhaltungsbedürfnis der Polizei unvereinbar. Der Kläger oder ein sonstiger potentieller Straftäter könnte sich andernfalls auf die Arbeitsweise der Polizei einstellen und sein Verhalten darauf einrichten.

Dieser Beurteilung ist zuzustimmen. Sie hat ihre gesetzliche Grundlage in Art. 48 Abs. 2 Ziff. 1 PAG. Danach unterbleibt die Auskunft, soweit eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei, zu besorgen ist. Die Besorgnis der Ausforschung muß sich aufgrund tatsächlicher Anhaltspunkte im konkreten Einzelfall ergeben, wobei die Richtung der Ausforschung über den konkreten Fall hinaus auf die Arbeitsweise der Polizei bei der Strafverfolgung und Verbrechensbekämpfung im allgemeinen bezogen sein kann. Liegt eine Ausforschungsabsicht erkennbar nicht vor, sind die gewünschten Auskünfte ihrer Art nach aber geeignet, die Arbeitsweise der Polizei zu gefährden, so hat die Auskunft nach Art. 48 Abs. 2 Ziff. 2 PAG zu unterbleiben. Diese Überlegung war

maßgebend für den Gesetzgeber, nur einen Anspruch auf Auskunft über die gespeicherten Daten zu gewähren.

Teilauskunft — Vollauskunft

Hat die Polizei über eine Person mehrere Informationen gespeichert und wünscht diese Person Auskunft **über alle** sie betreffenden Daten, dann hat die Polizei eine Vollauskunft zu erteilen. Soweit über einen Teil der Daten die Auskunft nach Art. 48 Abs. 2 PAG unterbleiben muß, erteilt die Polizei nur eine Teilauskunft. In diesem Fall darf die Auskunft — wie ich in einem Fall festgestellt habe — nicht als „Vollauskunft" bezeichnet werden. Sie darf auch ansonsten nicht den Eindruck einer vollständigen Auskunft erwecken. Vielmehr ist in der Entscheidung über das Auskunftsbegehren deutlich zu machen, daß dem Ersuchen nur teilweise entsprochen und im übrigen die Auskunftserteilung abgelehnt wurde. Der Betroffene ist darauf hinzuweisen, daß er sich an mich wenden kann. Darf jedoch der Betroffene aus den in Art. 48 Abs. 2 PAG genannten Gründen nicht erfahren, daß die Polizei noch weitere Informationen über ihn speichert, kann es sich empfehlen, die Auskunft insgesamt zu verweigern und den Betroffenen an den Landesbeauftragten zu verweisen (vgl. Nr. 4.14).

Auskunftsstelle Polizei

Immer wieder richten Bürger die Bitte an mich, ich möge ihnen Auskunft darüber erteilen, ob sie allgemein oder wegen eines konkreten Vorfalls bei der Polizei gespeichert sind. Richtiger Adressat eines derartigen Auskunftsersuchens ist jedoch die Polizei selbst. Dabei kann sich der Antragsteller entweder an die Polizeidienststelle, bei der er die Speicherung vermutet, die für den Wohnsitz des Bürgers zuständige Polizeidienststelle oder das Landeskriminalamt als gesetzlich bestimmte Zentralstelle für die polizeiliche Datenverarbeitung in Bayern wenden. Meine Zuständigkeit ist berührt, wenn Anhaltspunkte dafür vorliegen, daß Daten des Antragstellers zu Unrecht erhoben oder verarbeitet wurden. Gleiches gilt in den Fällen, in denen die Auskunftserteilung durch die Polizei im Einzelfall abgelehnt wird oder der Betroffene der Auskunft der Polizei mißtraut.

4.4 Allgemeine Prüfungen

Allgemeine Prüfungen habe ich im Berichtszeitraum bei folgenden Polizeibehörden vorgenommen:

- Landeskriminalamt
- Polizeipräsidium Oberbayern mit den Polizeidirektionen Fürstenfeldbruck, Ingolstadt und Traunstein
- Polizeipräsidium Schwaben mit den Polizeidirektionen Augsburg, Dillingen und Kempten
- Polizeipräsidium Niederbayern/Oberpfalz mit den Polizeidirektionen Passau, Regensburg und Weiden
- Polizeipräsidium München

Die Ergebnisse der Kontrollen lassen den Schluß zu, daß die Polizei die gesetzlichen und polizeiinternen Bestimmungen zur Datenerhebung und Datenverarbeitung im wesentlichen beachtet und Datenschutzverstöße die seltene Ausnahme sind.

4.4.1 Kriminalaktennachweis (KAN)

Meine Prüfungen des KAN haben wiederum gezeigt, daß die Polizei die Datenschutzbestimmungen **im wesentlichen beachtet** und einzelne Fehler die Ausnahme sind. Im Berichtsjahr habe ich insbesondere folgende Bereiche des KAN vor Ort stichprobenartig geprüft:

- Hausfriedensbruch und Hehlerei
- Verwendung von Kennzeichen verfassungswidriger Organisationen
- Verschiedene Straftaten gegen die sexuelle Selbstbestimmung wie Vergewaltigung, exhibitionistische Handlungen und Erregung öffentlichen Ärgernisses
- Straftaten gegen die Umwelt
- Straftaten eines ausgewählten Monats
- bestimmte Zeitpunkte für Aussonderungsprüfung

Die einzelnen Speicherungen, die ich nach den obengenannten Kriterien ausgewählt habe, habe ich nach folgenden Maßstäben geprüft:

- Ist die Speicherung rechtlich zulässig?
- Ist die „Speicherungsebene" richtig gewählt (Regional-, Landes-, Bundes-KAN)?
- Ist der Ausgang des Verfahrens in der Akte vermerkt? Wurde die Notwendigkeit einer Löschung oder einer Verkürzung der Speicherungsdauer im KAN geprüft? Ist die Prüfung dokumentiert?
- Wurden „personengebundene Hinweise" zu Recht vergeben, d.h. sind sie nach Aktenlage nachvollziehbar?
- Sind die Kriterien für die sog. KAN-Merker, die eine Straftat als überregional bedeutsam kennzeichnen und ihre Eingabe in den Bundes-KAN bewirken, nach Aktenlage nachvollziehbar?

Trotz der Vielzahl von Stichproben war nur in einem Fall eine Beanstandung auszusprechen. Die geringe Zahl und das geringe Gewicht der im übrigen festgestellten Fehler lassen den Schluß zu, daß sich der KAN bei den geprüften Polizeidienststellen aus datenschutzrechtlicher Sicht in einem zufriedenstellenden Zustand befindet.

In Einzelfällen fehlte der **Verfahrensausgang**. In anderen Fällen war aus der Kriminalakte nicht ersichtlich, weshalb personenbezogene Unterlagen **trotz Freispruchs** oder Verfahrenseinstellung weiter aufbewahrt wurden. In diesen Fällen haben nachträgliche

Prüfungen durch die speichernden Stellen entweder zur Löschung des Vorgangs aus dem KAN und zur Vernichtung der dazugehörenden Unterlagen oder zu einer nachträglichen plausiblen und nachvollziehbaren Begründung des verbleibenden polizeilichen Restverdachts geführt. In Fällen geringerer Bedeutung hat die Polizei Verkürzungen der Aussonderungsprüffristen vorgenommen.

4.5 Polizeipräsidium München

Im Berichtszeitraum habe ich wieder eine datenschutzrechtliche Prüfung beim Polizeipräsidium München vorgenommen. Folgende Bereiche wurden stichprobenartig geprüft:

- Anordnungen von besonderen Mitteln der Datenerhebung nach dem Polizeiaufgabengesetz (Art. 33 ff PAG),
- kriminalpolizeilicher Aktennachweis (KAN),
- Datei in einem Arbeitsplatzcomputer,
- verschiedene Karteien.

Die Prüfung wurde vor Ort bei verschiedenen Fachdienststellen durchgeführt.

4.5.1 Anordnungen von besonderen Mitteln der Datenerhebung

Die Anordnungsbefugnis für besondere Maßnahmen — ausgenommen die Anfertigung von Bildaufnahmen — steht nach Art. 33 Abs. 5 PAG den Leitern der Polizeidirektionen zu. Ihre Entscheidung wird darüber hinausgehend von der Einsatzabteilung geprüft, die auch die „personelle Koordination" der Einsätze und die zentrale Dokumentation der Anordnungen vornimmt. Bei den dort dokumentierten Maßnahmen handelt es sich **überwiegend um Observationen**, die vom PP München durchgeführt worden sind.

Erfreulich war die Feststellung, daß die gesetzlichen Voraussetzungen für den Einsatz der Maßnahmen in allen überprüften Fällen erfüllt waren, und zwar sowohl in materieller Hinsicht bezüglich der Zulässigkeit als auch in formaler Hinsicht bezüglich der Anordnungsbefugnis, der schriftlichen Abfassung der Anordnung und der Befristung der Maßnahmen (vgl. 4.3).

4.5.2 Kriminalpolizeilicher Aktennachweis (KAN)

Als Gesamtergebnis kann ich festhalten, daß die geringe Zahl und das geringe Gewicht der festgestellten Fehler den Schluß zulassen, daß das Polizeipräsidium München die Qualität des KAN aufgrund verstärkter Anstrengungen in den beiden letzten Jahren spürbar **verbessern** konnte.

Die **rückwirkende Erfassung** polizeilicher Kriminalakten im KAN war bereits im Juni 1990 abgeschlossen worden. Zu diesem Zeitpunkt bestanden noch ca. 185 000 Kriminalakten mit ca. 300 000 Vorgängen. Die Überarbeitung des Kriminalaktenbestandes beim Polizeipräsidium München nach den Richtlinien des KAN hat in der Zeit von 1984 bis 1990 zu einer Reduzierung um mehr als die Hälfte des ursprünglichen Bestandes geführt. Nebenher hat das Polizeipräsidium München den bereits erfaßten KAN-Bestand aufgrund früherer datenschutzrechtlicher Beanstandungen **überarbeitet**.

Stichproben aus dem Kriminalaktennachweis haben eine stark verbesserte Datenqualität erbracht. Gegenstand der Prüfung waren wie bei anderen Polizeidienststellen in erster Linie

- die Zulässigkeit der Speicherung nach den Regelungen für den KAN
- die Speicherungsebene (regional auf der Ebene des PP München, landesweit oder bundesweit)
- die Berücksichtigung des Verfahrensausgangs
- Fristverkürzungen bei Verfahrenseinstellungen
- personengebundene Hinweise.

In einigen Fällen mußte der **Ausgang des Strafverfahrens**, das zur Speicherung im KAN geführt hatte, nachgefordert werden. Die Ermittlung des Verfahrensausgangs und die Prüfung von Konsequenzen hieraus ist zunächst Sache des Polizeipräsidiums München und nicht des Landesbeauftragten. Dieser prüft erst daran anschließend, ob die Entscheidung der Polizei in Ordnung geht.

4.5.3 Datei in einem Arbeitsplatzcomputer

Die geprüfte Datei in einem Arbeitsplatzcomputer betraf die Arbeitsdatei einer Polizeidirektion, mit der die Bearbeitung polizeilicher Maßnahmen auf dem Oktoberfest unterstützt wird. Datenschutzrechtliche Bedenken gegen die Nutzung dieser Datei als Arbeitsdatei bestanden nicht.

4.5.4 Verschiedene Karteien

Kontrolliert wurde u.a. die Staatsschutzkartei. Die Speicherungen betrafen überwiegend Vorgänge, die als Straftaten auch im KAN enthalten waren. Der Staatsschutzbezug war in allen Fällen gegeben. Die übrigen Speicherungen betrafen Fälle der Gefahrenabwehr. Die gezogenen Stichproben waren nicht zu beanstanden.

4.6 Bayerisches Landeskriminalamt (BLKA)

Wie in den letzten Jahren habe ich beim BLKA in einer mehrtägigen Prüfung die Arbeitsdatei PIOS Innere Sicherheit (APIS) kontrolliert. APIS soll als Hilfsmittel zur Verhütung oder Aufklärung von Straftaten mit staatsfeindlicher Zielsetzung dienen, ist also keineswegs eine Terroristendatei, sondern eine **zentrale Staatsschutzdatei**.

Ansatzpunkte der Kontrolle waren bestimmte Erfassungszeiträume und Aussonderungsprüfdaten, der Straftatbestand „Hausfriedensbruch" und bestimmte Suchbegriffe wie „Wackersdorf", „Wiederaufarbei-

tungsanlage", „Atomkraft", „Linksextremismus" und „Rechtsextremismus". Ferner wurde eine Namensliste auf Bestand in APIS überprüft.

Als Ergebnis konnte ich feststellen:

- Die APIS-Prüfung 1991 ergab nur wenige Mängel, die zudem nicht gewichtig erscheinen. Daraus kann gefolgert werden, daß sich der vom BLKA zu verantwortende Datenbestand in datenschutzrechtlicher Hinsicht in einem guten Zustand befindet.
- Wie im letzten Jahr habe ich den Eindruck gewonnen, daß die **Speicherungsdauer** in geeigneten minderschweren Fällen auf drei oder fünf Jahre verkürzt wird.
- In einigen Fällen befand sich keine Mitteilung über den **Ausgang des Verfahrens** bei den Akten. Die Nachprüfungen ergaben, daß zum Teil das Verfahren noch nicht abgeschlossen war, im übrigen die Vorgänge mit Verurteilungen oder Einstellungen nach § 153 StPO endeten.
- Nur in wenigen Fällen war die APIS-Relevanz nicht klar ersichtlich. Bei der Nachprüfung ergab sich, daß die Speicherungen zwar grundsätzlich gerechtfertigt waren, wegen des nur geringen Verdachts einer staatsfeindlichen Zielsetzung jedoch eine **stark verkürzte Speicherungsdauer** angezeigt war. Die fraglichen Fälle wurden inzwischen gelöscht.

Da die Bewertung der APIS-Relevanz immer wieder Probleme aufwirft, habe ich im Beirat einige Zweifelsfälle vorgetragen. Im Beirat bestand Einvernehmen, daß die **Nichtanmeldung von Versammlungen** allein nicht ausreicht, um eine Speicherung in APIS zu rechtfertigen. Auch der Umstand, daß ein politisches Ziel mit der Demonstration verfolgt wird, reicht für eine APIS-Speicherung nicht aus, weil dies einer Versammlung regelmäßig immanent ist. Vielmehr muß vom BLKA jeweils sorgfältig geprüft werden, ob aus dem Motiv, der Verbindung des Täters zu einer Organisation oder wegen des Objekts der Verdacht begründet ist, daß staatsfeindliche Ziele verfolgt werden. In den überprüften Fällen war dieser Verdacht gering, so daß nur eine sehr kurze Aussonderungsprüffrist angemessen war (vgl. 4.8).

4.7 Kriminalaktennachweis (KAN) und Polizeiaufgabengesetz (PAG)

Der KAN gehört zu den in der polizeilichen Praxis wichtigsten Informationssammlungen für die Bewältigung der Aufgaben der Gefahrenabwehr, Gefahrenvorsorge und Aufklärung von Straftaten und Ordnungswidrigkeiten. Speicherungen im KAN sind in der Regel **besonders tiefe Eingriffe** in das informationelle Selbstbestimmungsrecht, weil der darin gespeicherte Bürger mit größerer Wahrscheinlichkeit als andere Bürger mit polizeilichen Maßnahmen rechnen muß. Deshalb muß der KAN, der bisher seine Grundlage in den bis zur Novellierung unzureichenden Vorschriften des PAG und in den KpS-Richtlinien hatte, alsbald an die neuen Vorgaben des PAG angepaßt werden. Mit diesem Ziel stehe ich seit Beginn des Jahres 1991 mit dem Innenministerium in Verhandlungen. Dabei geht es vornehmlich um die Reduzierung der im KAN zu speichernden Vorgänge, um die Verkürzung der Speicherfristen in Fällen von geringerer Bedeutung und um die Einschränkung der Fristenverlängerungsautomatik.

4.7.1 Reduzierung der KAN-Speicherungen

Nach Art. 38 Abs. 1 PAG kann die Polizei personenbezogene Daten u. a. in Dateien speichern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben **erforderlich** ist. Sie kann insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern, verändern und nutzen, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist (Art. 38 Abs. 2 PAG).

Im KAN sind Personen gespeichert, zu denen die Polizei eine Kriminalakte führt, sowie ein Hinweis zum Auffinden dieser Kriminalakte. Kriminalakten werden hauptsächlich angelegt, wenn die Polizei dem Verdacht einer Straftat oder Ordnungswidrigkeit nachgeht und hierzu Ermittlungen aufnimmt. Daneben werden in einer Kriminalakte Vorgänge festgehalten, in denen die Polizei eine sonstige Gefahr sieht, die in der Zukunft polizeiliche Abwehrmaßnahmen erfordern könnte. Seinen besonderen Eingriffscharakter erhält der KAN dadurch, daß Speicherungen über längere Zeit (10, 5 oder 2 Jahre) vorgehalten werden und in dieser Zeit von jeder angeschlossenen Polizeidienststelle, in bestimmten Fällen sogar bundesweit, abgefragt werden können.

Schon nach der geltenden Errichtungsanordnung für den KAN werden jedoch in Bayern nicht alle Kriminalakten in den KAN aufgenommen. Im KAN nicht gespeichert werden derzeit

- Verkehrsstraftaten (mit Ausnahme der in der Dienstanweisung KAN abschließend aufgezählten Delikte, z. B. vorsätzlicher gefährlicher Eingriff in den Straßenverkehr nach § 315 b StGB),
- Fahrlässigkeitsdelikte, die nur auf Antrag verfolgt werden,
- Privatklagedelikte, wenn der Geschädigte nach Hinweis den Privatklageweg beschreitet und auf eine Anzeigenerstattung bei der Polizei verzichtet,
- Verkehrsordnungswidrigkeiten,
- Straftaten nach § 218 Abs. 1 i.V.m. Abs. 3 StGB (Schwangerschaftsabbruch durch die Schwangere).

In diesen Fällen geht die Polizei zu Recht davon aus, daß eine Speicherung zur Erfüllung der Aufgaben der

Strafverfolgung und Gefahrenabwehr nicht erforderlich ist.

Die Aufnahme spezifischer Informationsregelungen in das PAG sollte jedoch zum Anlaß genommen werden, den Katalog der Straftaten und Ordnungswidrigkeiten gründlich zu durchforsten, ob unter dem Gesichtspunkt der Erforderlichkeit der Speicherung zur Gefahrenabwehr auf die Aufnahme weiterer Delikte in den KAN verzichtet werden kann, ohne daß die Erfüllung polizeilicher Aufgaben darunter leidet. In Betracht kommen hierzu folgende weitere Vorgänge:

- Privatklagedelikte, soweit von der Staatsanwaltschaft das öffentliche Interesse an der Anklageerhebung verneint wird,
- alle Fahrlässigkeitsdelikte,
- Ordnungswidrigkeiten, die bisher nur auf der Ebene der Polizeidirektionen, also regional gespeichert wurden.

Wenn die Staatsanwaltschaft bei einem Privatklagedelikt wie Hausfriedensbruch und Beleidigung das öffentliche Interesse an der Anklageerhebung verneint, sollte dies mit dem Verzicht auf die Anzeigenerstattung durch den Geschädigten gleichbehandelt werden. Wenn das öffentliche Interesse fehlt, dürfte von dem Beschuldigten, wenn überhaupt, nur eine zu vernachlässigende Gefahr für die öffentliche Sicherheit und Ordnung ausgehen, so daß polizeiliche Vorsorgemaßnahmen nicht erforderlich erscheinen. Bei den Fahrlässigkeitsdelikten kann nicht generell unterstellt werden, daß sich der Betroffene das Strafverfahren nicht zu Herzen nimmt und wieder straffällig wird. Es gibt auch keinen triftigen Grund, bei der Frage der Speicherung im KAN wie bisher zwischen Fahrlässigkeitsdelikten, die nur auf Antrag verfolgt werden, und anderen Fahrlässigkeitsdelikten zu unterscheiden. Ordnungswidrigkeiten, die bisher nur auf der Ebene der Polizeidirektionen gespeichert werden, haben so wenig kriminellen Gehalt, daß von einer relevanten Gefahr für die Zukunft in der Regel kaum gesprochen werden kann.

Sollten beim Innenministerium Bedenken gegen die vorgeschlagene Reduzierung des KAN bestehen, dann schlage ich vor, die Effizienz dieser von mir nicht für erforderlich gehaltenen Speicherungen in einem **Forschungsvorhaben** untersuchen zu lassen. Dabei könnte die Frage untersucht werden, in wievielen Fällen die fraglichen Speicherungen von der Polizei tatsächlich genutzt werden.

4.7.2 Verkürzung der Aussonderungsprüffristen

Für den KAN als automatisierter Datei sind nach Art. 37 Abs. 3 Satz 2 PAG Termine festzulegen, an denen spätestens überprüft werden muß, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist (Prüfungstermine). Diese Prüfungstermine dürfen nach Art. 38 Abs. 2 Satz 3 PAG im Normalfall bei Erwachsenen 10 Jahre, bei Jugendlichen 5 Jahre und bei Kindern 2 Jahre nicht überschreiten. In Fällen von geringerer Bedeutung sind kürzere Fristen festzusetzen (Art. 38 Abs. 2 Satz 4 PAG).

Der den Prüfungstermin festsetzende Sachbearbeiter hat bei der Speicherung eines jeden Vorgangs im KAN auch zu entscheiden, ob es sich um einen Fall von geringerer Bedeutung handelt. Ich halte es nicht für ausreichend, wenn er sich dabei nur an dem unbestimmten Gesetzesbegriff „Fall von geringerer Bedeutung" orientieren kann. Vielmehr sollten in der Errichtungsanordnung zum KAN oder in der Dienstanweisung weitere Fallgruppen gebildet werden, die in der Regel als solche von geringerer Bedeutung anzusehen sind. In Betracht kommen neben Straftaten von geringem Unrechtsgehalt auch kriminologische Gesichtspunkte (geringe kriminelle Energie, Ersttäter, Wiederholungsgefahr u. a.).

4.7.3 Einschränkung der Fristenverlängerungsautomatik

Die Prüfungsfrist, nach deren Ablauf spätestens überprüft werden muß, ob die suchfähige Speicherung der KAN-Eintragung weiterhin erforderlich ist, beginnt regelmäßig mit dem Ende des Jahres, in dem das letzte Ereignis erfaßt worden ist, das zur Speicherung der Daten geführt hat (Art. 38 Abs. 2 Satz 5 PAG). Die Verwaltungsvorschriften zum KAN sehen hierzu vor, daß die Speicherungsdauer bereits gespeicherter Ereignisse bei der Zuspeicherung eines weiteren Ereignisses regelmäßig verlängert wird, wenn die Laufzeit des neu zu speichernden Ereignisses das bereits festgelegte Aussonderungsprüfdatum übersteigt. Auf diese Weise können über Personen Vorgänge aus der Jugend- oder frühen Erwachsenenzeit bis ins Alter gespeichert sein. Begründet wird die Fristverlängerung für bereits gespeicherte Vorgänge mit dem Hinzutreten einer weiteren Speicherung damit, daß die Altvorgänge zur Gefahrenvorsorge insbesondere zur besseren Einschätzung des Betroffenen weiterhin erforderlich sind.

Ich meine, daß zumindest bei der Speicherung von Vermißtenfällen und Suizidversuchen von einer Verlängerung der Speicherungsdauer bereits gespeicherter Erkenntnisse abgesehen werden sollte. Darüber hinaus sollte generell die Speicherung von Suizidversuchen nach einem verkürzten Zeitraum von höchstens 2 Jahren auf ihre Notwendigkeit überprüft werden.

Die Stellungnahme des Innenministeriums zu diesen Fragen steht noch aus.

4.8 Arbeitsdatei PIOS Innere Sicherheit (APIS)

Die Datei APIS soll als Hilfsmittel zur Verhütung oder Aufklärung von Straftaten mit **staatsfeindlicher Zielsetzung** dienen. Dabei handelt es sich um Straftaten, die u.a. gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des

Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziele haben.

APIS wurde 1986 mit dem Ziel eingeführt, Informationen aus dem Bereich des Terrorismus und der sonstigen Staatsgefährdung zu sammeln und zu nutzen. Sie soll den Staatsschutzabteilungen der Polizei in Bund und Ländern ermöglichen, relevante Personen, Institutionen, Objekte, Sachen und Ereignisse sowie Zusammenhänge zwischen diesen zu erkennen und Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen zu gewinnen.

Auch 1991 wurde die datenschutzrechtliche Diskussion um APIS fortgesetzt.

4.8.1 Abschaffung von APIS

Zu Beginn des Berichtsjahres gab es unter den Datenschutzbeauftragten zunächst Bestrebungen, die Arbeitsdatei APIS generell in Frage zu stellen: Prüfungen der Datenschutzbeauftragten des Bundes und der Länder hätten deutlich gemacht, daß ein polizeilicher Nutzen zur Verhütung von Straftaten mit staatsfeindlicher Zielsetzung oder zur Abwehr von Gefahren — wenn überhaupt — nur mit großen Einschränkungen gegeben sei. Es sei festgestellt worden, daß zu viele Daten gespeichert seien, die für eine staatsfeindliche Motivation nichts hergäben. Mit solchen Informationen, die nicht zwischen Relevantem und Unbedeutendem unterschieden, könne keine zuverlässige Lagebeurteilung erstellt werden. Einem höchst fragwürdigen polizeilichen Nutzen von APIS stünden die Beeinträchtigung des informationellen Selbstbestimmungsrechts einer großen Zahl von Betroffenen gegenüber. Wegen der Schwierigkeiten bei der Bewertung von politischer Motivation durch die Polizei seien fehlerhafte Speicherungen vorprogrammiert.

Bewertung der Einwände gegen APIS

Die Datei APIS wäre unzulässig, wenn sie für die Erfüllung der polizeilichen Aufgaben der Verbrechensbekämpfung und Gefahrenabwehr im Bereich der Staatsschutzkriminalität untauglich, ungeeignet oder sonst nutzlos wäre. Doch davon kann nach dem derzeitigen Erkenntnisstand keine Rede sein. Weder hat die in einem Bundesland bisher von der Polizei durchgeführte Untersuchung die Nutzlosigkeit von APIS ergeben, noch könnte die Untersuchung in einem einzigen Land eine tragfähige Grundlage für ein derartiges Urteil abgeben. Bei meinen Prüfungen von APIS haben sich zwar immer wieder Meinungsverschiedenheiten darüber ergeben, ob in einem bestimmten Verhalten Anzeichen staatsfeindlicher krimineller Aktivitäten gesehen werden können. Doch kann wegen solcher Meinungsunterschiede in Einzelfällen nicht der Nutzen der ganzen Datei in Frage gestellt werden.

Selbstverständlich muß die Polizei die Nützlichkeit der Datei APIS bei der Erfüllung ihrer Aufgaben plausibel belegen können. Anläßlich eines Informationsbesuchs beim Bayer. Landeskriminalamt konnte ich mich davon überzeugen, daß die Polizei das Hilfsmittel APIS intensiv nutzt. Wenngleich wohl der Nutzen von APIS angesichts der Fahndungsdefizite im terroristischen Bereich hinter den Erwartungen zurückbleibt, so wird dadurch nicht APIS als Ganzes in Frage gestellt, zumal das Ausbleiben von Fahndungserfolgen gegen die RAF auf eine ganze Reihe von Ursachen zurückzuführen sein dürfte. Hinzu kommt, daß die Effektivität von APIS gerade unter dem mangelhaften Vollzug in zahlreichen Ländern leidet, der einen bundesweiten Überblick über APIS-relevante Vorgänge nicht mehr erlaubt.

4.8.2 Reduzierung der Speicherungen in APIS

Eine Reihe von Ländern ist dazu übergegangen, künftig nur noch die schweren typischen Staatsschutzdelikte oder terroristischen Gewalttaten und die diesen vergleichbaren Straftaten mit politischem Hintergrund in APIS aufzunehmen, die anderen Staatsschutzdelikte hingegen in landeseigene Informationssysteme zu übernehmen. Teilweise stellen die Kriminalämter auf die Schwere und die überörtliche Bedeutung der Tat ab.

Im 12. Tätigkeitsbericht habe ich von der Kritik einiger Datenschutzbeauftragter berichtet, der Erfassungstatbestand „andere Straftaten mit staatsfeindlicher Zielsetzung" nehme im Vergleich zu den typischen Staatsschutzdelikten, den sog. Katalogstraftaten, den größten Teil der Speicherungen in APIS (70 bis 90 v.H.) ein; deshalb müßten APIS-Speicherungen eingeschränkt werden.

Reduzierungen von APIS-Speicherungen können nach meiner Auffassung nicht unter dem Gesichtspunkt der Verhältnismäßigkeit der Mittel gefordert werden. Maßgeblich für die Speicherung ist die staatsfeindliche Motivation des Täters, nicht die Schwere der Straftat oder die überörtliche Begehung. Von Straftaten mit staatsfeindlicher Zielsetzung sollte angesichts der heutigen Mobilität der Gesellschaft nicht nur die Polizei eines Landes, sondern alle Länderpolizeien informiert sein. Im übrigen führt die in einer Reihe von Ländern praktizierte Reduzierung der APIS-Speicherungen dazu, daß Straftaten mit zweifellos staatsfeindlicher Zielsetzung für die Lagebeurteilung nicht mehr bundesweit zur Verfügung stehen. Täter mit staatsfeindlicher Zielsetzung können sich durch Umzug in ein anderes Bundesland den Ermittlungen des Staatsschutzes ohne größere Schwierigkeiten entziehen. Wenn die Polizei aus Gründen der inneren Sicherheit das Abtauchen von Personen, die eine Gefahr für die innere Sicherheit darstellen können, durch bundesweites Bereithalten von Informationen über diesen Personenkreis verhindern will, kann in der Speicherung dieses Personenkreises in ei-

ner Verbunddatei kein Verstoß gegen den Verhältnismäßigkeitsgrundsatz gesehen werden.

Das Landeskriminalamt hat auf meine Bitte seine Speicherungen daraufhin überprüft, wie hoch der Anteil der typischen Staatsschutzdelikte und der anderen Delikte mit staatsfeindlicher Zielsetzung ist. Nach den ermittelten Zahlen beträgt 1990 der Anteil der typischen Staatsschutzdelikte in Bayern 63 v.H., und derjenige der sog. anderen Straftaten, bei denen sich die staatsfeindliche Zielsetzung erst aus dem Motiv des Täters, seiner Verbindung zu staatsfeindlichen Organisationen oder aus dem angegriffenen Objekt ergibt, nicht 90 v.H. sondern nur 37 v.H. Die Kritik, APIS sei wegen des unverhältnismäßig hohen Anteils sog. anderer Straftaten an den Gesamtspeicherungen vom Ansatz her falsch konzipiert, erscheint mir bei dem festgestellten Zahlenverhältnis widerlegt.

4.8.3 Erweiterung von APIS

Als nach dem Attentat auf den Chef der Treuhandanstalt Dr. Rohwedder am 1. April 1991 wieder einmal die Fahndungsdefizite der Polizei im terroristischen Bereich ins öffentliche Bewußtsein rückten, wurde auch der **Datenschutz als Sündenbock** für diese Defizite ausfindig gemacht. Überprüft werden müßten die **zu weitreichenden Löschungsverpflichtungen**, die es der Polizei unmöglich machten, die kriminellen Lebensläufe von Terroristen frühzeitig zu erkennen und geeignete Fahndungsansätze zu finden. Zu APIS wurde gefordert, die Speicherungshöchstdauer in Fällen von geringer Bedeutung (bisher 3 Jahre) anzuheben und die Speicherdauer von Kontaktpersonen wesentlich zu erweitern.

Selbstverständlich ist es legitim, nach fünf Jahren Erfahrung mit APIS zu prüfen, welche Änderungen notwendig sind, um den Nutzen dieser Datei für die Polizei zu steigern. Die Verlängerung von Speicherfristen halte ich für möglich, wenn vernünftige und begründete Vorschläge eingebracht werden. Allerdings sollte die Überprüfung auf der Grundlage der bisherigen Erfahrungen keine Einbahnstraße in Richtung mehr und längerfristige Speicherungen sein. Vielmehr sollte APIS — wie auch alle anderen Dateien — zu gegebener Zeit auf ihre Nützlichkeit, Eignung und Erforderlichkeit im ganzen wie in den einzelnen Bestimmungen überprüft werden.

4.9 Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung — Verbrechensbekämpfung" (PSV)

Im Jahr 1988 hat das Innenministerium die Datei „Vorgangsverwaltung" mit Errichtungsanordnung zugelassen. Diese Datei wird derzeit vom Polizeipräsidium München für den Ballungsraum München, vom Polizeipräsidium Mittelfranken für den Ballungsraum Nürnberg/Fürth/Erlangen sowie von einigen Polizeidirektionen betrieben. Zweck der Datei ist es, die Bearbeitung polizeilich relevanter ermittlungs- und verwaltungstechnischer Vorgänge zu unterstützen.

Einige Eingaben, die Speicherungen in der Datei „Vorgangsverwaltung" betrafen, gaben Anlaß, die Verwendung der Datei näher zu überprüfen. Zu klären waren dabei insbesondere die zulässigen **Verwendungszwecke**, das **Verhältnis** der Datei „Vorgangsverwaltung" zu anderen Dateien sowie die zulässigen **Speicherungsfristen**. Im Laufe des Jahres 1991 begann dann auch der „Arbeitskreis Sicherheit" der Datenschutzbeauftragten, sich mit der Vorgangsverwaltung zu beschäftigen. Das Innenministerium überarbeitete schließlich die bisherige Errichtungsanordnung und übersandte mir einen Entwurf für die künftige Datei „Polizeiliche Sachbearbeitung/Vorgangsverwaltung — Verbrechensbekämpfung" (PSV).

4.9.1 Dateibeschreibung

Zweck und Inhalt von PSV:

Die PSV soll die **Grundlage des Informationssystems** der Bayerischen Polizei (IBP) werden.
Zweck der PSV ist
- die innerdienstliche Verwaltung des Vorgangs,
- die Ermittlungshilfe für Zwecke der Verbrechensbekämpfung,
- die Gewinnung von Entscheidungshilfen für innerbetriebliche Aufgaben,
- die Bereitstellung von einsatztaktischen und logistischen Daten,
- die Bereitstellung von Informationselementen für andere IBP-Anwendungen,
- die Dokumentation.

Inhalt

Zur Erfüllung dieser Zwecke werden alle Vorgänge in der PSV gespeichert, die bei den Polizeidienststellen eines bestimmten Zuständigkeitsbereichs in Wahrnehmung ihrer gesetzlichen Aufgaben anfallen. Zu den Speicherungen müssen schriftliche Unterlagen vorhanden sein.

Im wesentlichen sind folgende Vorgänge aufzunehmen:
- Strafanzeigen,
- Ordnungswidrigkeitenanzeigen (ausgenommen Verkehrsordnungswidrigkeiten),
- Verkehrsunfallanzeigen,
- sonstige schriftliche Vorgänge, die polizeiliche Ermittlungen oder Maßnahmen auslösen oder ausgelöst haben oder die für den polizeilichen Aufgabenbereich von Belang sind und eine Dokumentation erfordern.

Betroffener Personenkreis

Von Speicherungen in der PSV ist ein **wesentlich größerer Personenkreis** als von Speicherungen im Kriminalaktennachweis betroffen, der überwiegend nur personenbezogene Daten von Beschuldigten und

Verdächtigen in Strafverfahren oder von Betroffenen in Ordnungswidrigkeitenverfahren enthält.

In der neu definierten Datei können Daten über folgende Personen gespeichert werden:
- Beschuldigte, Tatverdächtige, Verurteilte,
- Betroffene und Beteiligte i. S. des Ordnungswidrigkeitenrechts,
- von polizeilichen Maßnahmen Betroffene,
- Verantwortliche, Beauftragte und Dritte nach Art. 7 bis 10 PAG,
- Personen, über die Auskunftsersuchen aufgrund besonderer Rechtsvorschriften bei der Polizei gestellt worden sind,
- Opfer, Verletzte, Strafantragsberechtigte,
- Geschädigte, Anzeigeerstatter, Mitteiler, Verkehrsunfallbeteiligte,
- sonstige Personen, deren Daten zur Erfüllung der polizeilichen Aufgaben vorgehalten werden müssen,
- Beschäftigte der Polizei.

Eingabe-, zugangs-, abfrage- und rechercheberechtigt sind nur die bayerischen Polizeivollzugsbeamten und sonstige Bedienstete kraft besonderen Auftrags. **Auskünfte** an Stellen außerhalb des Polizeibereichs dürfen grundsätzlich nur aus schriftlichen Unterlagen erteilt werden.

Die **Aussonderungsprüffristen** und die **Speicherungsdauer** für Strafanzeigen gegen bekannte Täter und Störer knüpfen grundsätzlich an die Fristen im Kriminalaktennachweis an.

4.9.2 Datenschutzrechtliche Bewertung der PSV

1. Festgelegte Dateizwecke

   Gegen die Festlegung mehrerer Dateizwecke (Vorgangsverwaltung, Dokumentation, Gefahrenabwehr einschließlich Gefahrenvorsorge und -vorbeugung, Verbrechensbekämpfung) bestehen keine grundsätzlichen Einwände. Der Grundsatz der **Zweckbindung**, der zum Inhalt hat, daß Daten, die zu einem bestimmten Zweck erhoben worden sind, für andere Zwecke nur im gesetzlich gestatteten Rahmen verwendet werden dürfen, wird durch eine Datei, die mehreren Zwecken dient, nicht berührt. Eine solche Datei ist nicht anders zu bewerten als ein mehreren Zwecken dienender schriftlicher Vorgang.

   Eine **Aufteilung** der polizeilichen Sachbearbeitung auf **mehrere Dateien mit verschiedenen Zwecken** oder auf mehrere gegeneinander abgeschottete Teile einer Datei (physikalisch gesonderte Speicherung) ist auch nicht etwa deshalb geboten, weil für manche polizeilichen Informationen Verwertungsverbote oder -beschränkungen bestehen. **Nutzungsbeschränkungen**, z. B. aufgrund einer Sperrung, kann, soweit erforderlich, durch technisch-organisatorische Vorkehrungen Rechnung getragen werden. Andernfalls bestünde die Gefahr, daß der polizeiliche Informationsbestand in mehrere gegeneinander abgeschottete „Schubladen" verteilt würde und eine **Zusammenführung und Verknüpfung polizeilicher Erkenntnisse**, die beispielsweise zur Verbrechensbekämpfung oder zur Gefahrenabwehr erforderlich sind, vielfach unmöglich wären. Die automatisierte Datenverarbeitung darf nicht dazu führen, daß sich die Polizei künstlich unwissend macht.

2. Erforderlichkeit automatisierter Speicherung

   Nach dem Entwurf der Errichtungsanordnung sollen eine Reihe von Vorgängen wie Auskunftsersuchen nach Verwaltungsdaten und negativ beantwortete Erkenntnisanfragen grundsätzlich nicht gespeichert werden.

   Entsprechend der Praxis bei manchen Polizeidienststellen habe ich gefordert, daß Vorgänge, die sich nach polizeilicher Erfahrung innerhalb kurzer Zeit völlig und ohne Nachwirkungen erledigen, **nicht automatisiert in der PSV** und damit auf 5 Jahre gespeichert, sondern überhaupt nicht in die PSV aufgenommen werden. So erhält die Polizei von der Ordnungsbehörde (Kreisverwaltungsbehörde, Landratsamt) z. B. Abdrucke von Sondernutzungsgenehmigungen für politische Info-Stände, von Anzeigen für öffentliche Versammlungen unter freiem Himmel oder Genehmigungen von Radsportveranstaltungen. Nach der Durchführung der Veranstaltung, bei der die Polizei ggf. zu prüfen hat, ob die Gesetze, insbesondere die Auflagen, eingehalten werden, ist der Vorgang in aller Regel erledigt. Die schriftlichen Unterlagen können nach wenigen Wochen vernichtet werden. Hier wäre eine automatisierte jahrelange Speicherung unverhältnismäßig. **Ausnahmen** müssen allerdings gelten, wenn beispielsweise solche öffentlichen Veranstaltungen von Extremisten durchgeführt werden. Über das öffentliche Treiben dieser Personen informiert zu sein, gehört zu den Aufgaben der Polizei, nicht nur des Verfassungsschutzes.

3. Verhältnis der PSV zu anderen Dateien

   Eine Strafanzeige wird als Vorgang in die PSV eingetragen. Wird danach im Zuge der weiteren Sachbearbeitung eine Kriminalakte angelegt, kommt es auch zur Eintragung im Kriminalaktennachweis (KAN). Sofern erkennungsdienstliche Maßnahmen durchgeführt werden, folgt die Eintragung in die ED-Datei.

   Solange der Verdächtige im KAN gespeichert ist, bestehen gegen die Nutzung der PSV-Eintragung zu Recherchezwecken keine Bedenken. Entgegen manchen Behauptungen gibt es **kein Verbot der Doppelspeicherung** oder gleichzeitigen Nutzung von KAN und PSV. Die Speicherung im KAN be-

wirkt kein Nutzungsverbot der PSV zur Verbrechensbekämpfung. Sobald jedoch die KAN-Eintragung gelöscht oder gesperrt ist, darf auch die PSV-Eintragung für Zwecke der Verbrechensbekämpfung nicht mehr zur Verfügung stehen. Zu weitgehend erschiene mir die Forderung, bei einer Löschung im KAN auch die Löschung in der PSV herbeizuführen, da es durchaus denkbar ist, daß der Vorgang noch für die Durchsetzung von Schadenersatzansprüchen oder für Disziplinarmaßnahmen sowie zur Dokumentation polizeilichen Handelns benötigt wird.

4. Beschränkung der Zugangsberechtigung

   Zugriff zu den Informationen der PSV dürfen nur die Polizeibeamten erhalten, die den Dateizugang zur Erfüllung ihrer polizeilichen Aufgaben benötigen.

   Da die PSV auch der Verbrechensbekämpfung dient, erscheint es zweckmäßig, bei der Definition des Umfangs der Zugangsberechtigung in räumlicher Hinsicht auf **kriminal-geographische Räume** abzustellen. Aus der Sicht des Datenschutzes sollten diese Räume möglichst klein bleiben. Die Beschränkung auf die Bediensteten einer Polizeiinspektion oder einer Polizeidirektion würde jedoch je nach den Umständen die kriminalistischen Möglichkeiten, welche die PSV bietet, zu stark einschränken und scheint mir deshalb nicht zwingend geboten.

   Entschieden zu weit geht die Forderung, in laufenden Verfahren nur den Mitarbeitern der sachbearbeitenden Stelle Zugriffsberechtigung einzuräumen. Das würde die Zusammenführung sachlich zusammengehörender Vorgänge verhindern und die bestehende Verbindung von Vorgängen nicht erkennen lassen. Außerdem bestünde die Gefahr, daß ein Vorgang doppelt bearbeitet würde. Eine Anzeige eines Opfers könnte u. U. nicht mit dem Verfahren gegen den Täter zusammengeführt werden.

   Zu erwägen ist jedoch, ob innerhalb eines größeren Zugangsbereiches dem einzelnen Sachbearbeiter in geeigneten Fallgruppen die Möglichkeit eingeräumt werden kann, entsprechend den konkreten Notwendigkeiten den Umfang des Lesezugriffs anderer Bediensteter einzuschränken.

   Für bestimmte Vorgänge, bei denen ganz besonders sensible Daten gespeichert werden, erscheint mir eine enge Zugriffsbeschränkung notwendig.

   Außerdem sollten auf Vorgänge, die der Verbrechensbekämpfung nicht mehr zur Verfügung stehen, sondern nur mehr im Rahmen der Vorgangsverwaltung oder Dokumentation verwendet werden dürfen, nur noch der Vorgangsverwalter und bestimmte Bedienstete Zugriff haben.

5. Beschränkungen der Recherchemöglichkeiten

   In der PSV sind im Gegensatz zum KAN, in dem nur Straftäter und sonstige Störer suchfähig gespeichert sind, zahlreiche andere Personengruppen suchfähig gespeichert. Bei der Recherche nach einem bestimmten Namen erscheinen in der PSV alle Vorgänge, in denen die abgefragte Person mit Polizeidienststellen zu tun hatte, für die eine gemeinsame PSV eingerichtet ist. Bei einer Namensrecherche kann der Betroffene als Straftäter, Finder, Obdachloser, Ruhestörer, Vermißter, Prostituierte etc. auftauchen.

   Deshalb ist von Datenschutzbeauftragten erwogen worden, Namensabfragen nur über einen aus mehreren Merkmalen **zusammengesetzten Suchbegriff** (Namen, Beteiligungsart, Bearbeitungszweck, Strafvorwurf) zuzulassen. Durch eine solche Beschränkung würde jedoch die polizeiliche Sachbearbeitung ganz erheblich erschwert. Die Vorteile der automatisierten Datenverarbeitung würden weitgehend zunichte. Dem berechtigten Anliegen, dem Polizeibeamten nur die notwendigen Daten zur Verfügung zu stellen, kann wohl nur durch Zugangsbeschränkungen Rechnung getragen werden.

6. Protokollierung

   Wenn zahlreiche Bedienstete auf eine Datei mit vielfach verwertbaren Informationen zugreifen können, besteht zwangsläufig die **Gefahr des Mißbrauchs**. Deshalb werden in Bayern seit 1989 alle Abrufe aus IBP-Dateien und aus ZEVIS beim Landeskriminalamt und teilweise bei den Polizeipräsidien protokolliert.

   Eine solche Protokollierung halte ich auch für PSV-Abfragen für **unumgänglich**. Jeder Zugriff auf die PSV-Daten ist für eine bestimmte Zeit, in der effektive Kontrollen möglich sind, mit dem jeweiligen Abfragegrund zu protokollieren. Andernfalls könnte die bisherige Protokollierung problemlos unterlaufen werden, indem Abfragen im IBP durch Nutzung der PSV ersetzt werden. Je mehr Zugriffsmöglichkeiten, desto mehr Nutzungskontrollen!

Eine abschließende datenschutzrechtliche Bewertung der neuen Datei PSV ist mir derzeit noch nicht möglich. Hierzu möchte ich die Beratungen im Arbeitskreis „Sicherheit" auswerten.

4.10 Datei „Gewalttäter Sport"

Seit längerem wird von der polizeilichen Praxis, aber auch von Politikern, dem Deutschen Fußballbund sowie Teilen der Medien die Einrichtung einer **bundesweiten Datei** über Personen gefordert, die wegen **Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen** in Erscheinung getreten sind. Auch die unab-

hängige Regierungskommission zur Verhinderung und Bekämpfung von Gewalt hält eine Informations- und Datensammlung durch die Polizei und den Informationsaustausch zwischen den Polizeibehörden der Bundesländer zur Bekämpfung der Gewalttätigkeiten bei Sportveranstaltungen für erforderlich. Die Konferenz der Innenminister des Bundes und der Länder hat im Dezember 1990 einen Arbeitskreis beauftragt zu prüfen, ob und in welcher Form von den Polizeien des Bundes und der Länder Informationen über Personen, die wegen Gewalttätigkeiten im Zusammenhang mit sportlichen Veranstaltungen in Erscheinung getreten sind, zur Gefahrenabwehr und zur Verfolgung von Straftaten vorgehalten und genutzt werden können.

Als vorläufiges Ergebnis des Arbeitskreises liegt mir ein polizeiinternes **Arbeitspapier** vor, das die Erforderlichkeit einer bundesweiten Datei „Gewalttäter Sport" aus polizeilicher Sicht begründet und Vorschläge zum Inhalt und zur Nutzung der Datei enthält.

Auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1991 wurde die geplante Datei intensiv und kontrovers erörtert. Die Datenschutzbeauftragten waren der Ansicht, daß eine abschließende Meinungsbildung nach dem derzeitigen Informationsstand noch nicht möglich ist.

Nach Gesprächen mit dem Innenministerium und Praktikern aus den Polizeipräsidien München und Mittelfranken und nach Erörterung in der Datenschutzkonferenz bin ich der Auffassung, daß die Eignung und Erforderlichkeit der geplanten Datei zumindest soweit dargetan sind, daß die Datei zunächst für einen Zeitraum von zwei bis drei Jahren in der Praxis erprobt werden kann. Dabei dürfen an die Eignung und Erforderlichkeit der Datei zur Vorbeugung und Bekämpfung von Gewalttätigkeiten vor, während und nach Sportveranstaltungen mit Zuschauern aus den Zuständigkeitsbereichen anderer Landespolizeien keine überzogenen Anforderungen gestellt werden. Wer verlangt, daß mit dieser Verbunddatei das Problem gelöst ist, erwartet sich von einer Datei zu viel. Sie kann nur **Hilfsmittel** sein für polizeiliche Maßnahmen wie Begleitung, Beobachtung von Fan-Gruppen vom Eintreffen bis zur Abreise, Einsatzplanung, Kräfteeinsatz, Gewahrsam, Platzverweis u.a. Brutale Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen sind nicht das geeignete Feld, wo man Informationsdefizite bewußt in Kauf nehmen sollte. Angesichts verheerender Ausschreitungen deutscher „Fußballfans" in Brüssel am 20. November 1991 sind ängstliche Zweifel an der Eignung der Datei unangebracht.

Aus meiner Sicht bestehen keine datenschutzrechtlichen Bedenken gegen eine Verbunddatei „Gewalttäter Sport", wenn insbesondere folgende Forderungen berücksichtigt werden:

1. Aufbau und Betrieb einer solchen Datei müssen die jeweils geltenden gesetzlichen Bestimmungen beachten.

   Der Betrieb erfordert den Online-Abruf von Informationen aus der Verbunddatei. In einzelnen Ländern (u.a. Berlin, Bremen, Hamburg, Hessen, Saarland) ist für die Beteiligung an der Datei „Gewalttäter Sport" ein **Sondergesetz** erforderlich.

2. In einer Verbunddatei von Bund und Ländern sollen nur diejenigen Daten gespeichert werden, die zur Bekämpfung (Verhütung und Aufklärung) von Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen benötigt werden. In Betracht kommt dabei insbesondere die Speicherung von Straftaten, polizeilicher Gewahrsamnahme, Stadionverboten, Sicherstellung und Beschlagnahme von Waffen oder anderen Gegenständen im Zusammenhang mit Sportveranstaltungen, wenn anzunehmen ist, daß der Betroffene mit Gewalttätigkeiten im Zusammenhang mit Sportveranstaltungen wieder in Erscheinung treten wird.

3. Die Speicherung der Daten in einer **Verbunddatei** ist auf die Personen zu beschränken, von denen anzunehmen ist, daß sie als **„reisende Gewalttäter"** bei Sportveranstaltungen in Erscheinung treten. Die in Betracht kommenden Straftaten sollten darüber hinaus in einem Katalog aufgeführt werden.

4. Werden die Daten wegen eines eingeleiteten Ermittlungsverfahrens aufgrund einschlägiger Straftaten gespeichert, so sind sie zu löschen, wenn der dem Ermittlungsverfahren zugrundeliegende Verdacht entfallen ist.

5. Den Betroffenen beschreibende personenbezogene **Merkmale** dürfen nur anhand eines festgelegten Katalogs gespeichert werden.

6. Es sollte geprüft werden, ob dem Bundesgrenzschutz — über die allgemeinen Zugriffsmöglichkeiten hinaus — ein besonders gekennzeichneter Bestand **„international tätiger Gewalttäter"** zur Verfügung gestellt werden kann.

7. Zugriffe auf die Datei sind auf Landesebene zentral zu **protokollieren**.

8. **Übermittlungen** aus der Datei an die Betreiber von Sportstätten können nur dann in Betracht kommen, wenn die Polizei selbst keine oder keine hinreichenden Maßnahmen zur Gefahrenabwehr ergreifen kann. Ein Direktanschluß der Betreiber ist auszuschließen. Im übrigen richtet sich die Übermittlung von Erkenntnissen aus den Akten nach dem jeweiligen Landespolizeirecht.

9. Die Speicherung ist grundsätzlich nach 2 Jahren zu überprüfen. Bei Beteiligung an schweren Ausschreitungen kann eine längere **Speicherfrist** festgesetzt werden.

Während über die Verbunddatei „Gewalttäter Sport" noch diskutiert wird, hat das PP München eine Datei „Straftaten bei Sportveranstaltungen und gewalttätige Jugendgruppen" eingerichtet (vgl. Nr. 4.11).

4.11 Datei „Straftäter bei Sportveranstaltungen und gewalttätige Jugendgruppen"

Wegen des besorgniserregenden Anstiegs der jugendspezifischen Gewalttaten und der Gewaltdelikte im Zusammenhang mit Sportveranstaltungen hat das Innenministerium der Errichtung einer bayerischen Arbeitsdatei „Straftäter bei Sportveranstaltungen und gewalttätige Jugendgruppen" zugestimmt. In der Errichtungsanordnung wird festgelegt, daß Daten aus dieser Datei mittels **Online-Anschluß** an die für die **Verfolgung** von Straftaten und Ordnungswidrigkeiten im Zusammenhang mit Sportveranstaltungen sowie jugend- und gruppentypischer Gewalttaten zuständigen Polizeidienststellen übermittelt werden können.

Die bisher bei den Fachdienststellen geführten Karteien über jugendtypische Gewalttäter und Mitglieder gewalttätiger Gruppen waren dem Informationsbedarf der Sachbearbeiter aufgrund der fehlenden Auswertungsmöglichkeiten nicht gewachsen. Gerade bei der Bekämpfung des Fußballrowdytums und der oftmals durch Jugendbanden begangenen Gewaltdelikte ist es jedoch unabdingbar, das **Personengefüge** der Gruppen und die **personellen Zusammenhänge** in den gewaltbereiten Fanclubs zu durchdringen, Neugründungen von „Blasen" zu erkennen und so Zusammenhänge innerhalb dieser Szene herzustellen. Diese Informationszusammenhänge, die sich aus den bisher bestehenden Karteien, den Kriminalakten, den Lichtbildsammlungen, der Personenbeschreibung einzelner Täter, den Vorgangsabdrucken der Sachbearbeiter und nicht zuletzt aus dem Erfahrungs-, Personen-, Milieu- und Tatwissen der eingesetzten Beamten zusammensetzten, waren bisher weder zu gewinnen noch zu verwalten oder auszuwerten.

In der Datei werden Daten über folgende Personen erfaßt:
- Personen, gegen die wegen Straftaten und Ordnungswidrigkeiten im **Zusammenhang mit Ausschreitungen** bei Sportveranstaltungen ermittelt wurde,
- Personen, gegen die Maßnahmen nach dem Jugendgerichtsgesetz gerichtet werden und gegen die wegen **jugend- und gruppentypischer Agressionsdelikte** (insbesondere Vandalismus, alle Formen der Körperverletzung, Sittlichkeitsdelikte, Raub und räuberische Erpressung, Tötungsdelikte) polizeilich ermittelt wurde,
- Personen, die aufgrund glaubwürdiger Hinweise oder polizeilicher Ermittlungen gewalttätigen Gruppierungen oder deren engerem Umfeld zuzuordnen sind, gegen die aber noch nicht wegen Straftaten und Ordnungswidrigkeiten polizeiliche Ermittlungen geführt werden.
  Personen, die dem letztgenannten Personenkreis zuzuordnen sind, werden allerdings nur dann in der Datei erfaßt, wenn sie im örtlichen Zuständigkeitsbereich der jeweiligen Polizeidienststelle wohnen, sich dort über einen längeren Zeitraum aufhalten oder von außerhalb zuziehen.

Die Datei wird bisher von den Polizeipräsidien München und Oberbayern bei sportlichen Großveranstaltungen eingesetzt.

Eine abschließende Bewertung der Datei ist erst nach einer Prüfung vor Ort möglich.

4.12 Berücksichtigung des Verfahrensausgangs

Mitteilung des Verfahrensausgangs

In früheren Jahren habe ich bei datenschutzrechtlichen Prüfungen häufig festgestellt, daß sich in der polizeilichen Kriminalakte keine Mitteilung über den Ausgang des Strafverfahrens befand, obwohl dieses längst abgeschlossen war. Zu diesem Punkt konnte ich bei meinen Prüfungen im Berichtszeitraum jedenfalls in neueren polizeilichen Unterlagen erhebliche **Verbesserungen** feststellen. Nur in Einzelfällen befand sich die erforderliche Mitteilung der Staatsanwaltschaft nicht bei der Kriminalakte.

Hinweis auf Wegfall des Tatverdachts bei Einstellung

Bei Einstellung des Verfahrens nach **§ 170 Abs. 2 StPO** ist zusätzlich zur Mitteilung der Einstellung ein Hinweis für die Polizei erforderlich, ob der Tatverdacht entfallen ist. Erst durch diesen Hinweis wird die Polizei in die Lage versetzt, mit vertretbarem Aufwand das Ergebnis des Justizverfahrens bei der Entscheidung über die weitere Speicherung personenbezogener Daten in polizeilichen Dateien und Akten zu berücksichtigen.

Landtagsbeschluß vom 15. Mai 1991

Auf meine Anregung hin hat der Bayer. Landtag (Drs. 12/1498) die Staatsregierung gebeten, die Führung kriminalpolizeilicher Sammlungen dadurch zu verbessern, daß
- die Staatsanwaltschaften die „Mitteilungen von Verfahrensausgängen" bei der Justiz durch geeignete organisatorische Vorkehrungen sicherstellen,
- bei Verfahrenseinstellungen aus der Mitteilung hervorgeht, ob nach Auffassung der Staatsanwaltschaft damit auch der Tatverdacht entfallen ist.

Während das Justizministerium die Mitteilung des Verfahrensausgangs durch allgemeine Dienstbesprechungen sichergestellt hat und die Generalstaatsan-

wälte in einer Dienstbesprechung beschlossen haben, den Vollzug von Nr. 11 MiStra regelmäßig zu prüfen, zeichnet sich zu meiner Forderung, daß bei Einstellungen nach § 170 Abs. 2 StPO aus der Mitteilung auch hervorgehen soll, ob nach Auffassung der Staatsanwaltschaft der Tatverdacht entfallen ist, keine Lösung ab. Das Justizministerium hat Bedenken gegen eine Mitteilung „erster" oder „zweiter" Klasse. Es verweist darauf, daß entsprechende gesetzliche Mitteilungspflichten in der StPO fehlen. Die StPO lehne bei Einstellungen und Freisprüchen eine Unterscheidung zwischen Unschuld und fortbestehendem Verdacht bewußt ab.

Aus meiner Sicht stehen dem von mir geforderten Hinweis rechtliche Gründe nicht entgegen, da es sich nicht um die Mitteilung belastender, sondern für den Betroffenen günstiger Umstände handelt. Sollte die Justiz an ihrem Standpunkt festhalten, wird **in jedem Fall einer Verfahrenseinstellung** nach § 170 Abs. 2 StPO ebenso wie bisher bei einem Freispruch die **Übersendung der Entscheidungsgründe an die Polizei notwendig** sein, auch wenn damit ein erheblicher zusätzlicher Arbeitsaufwand für die Polizei verbunden ist.

4.13 Speicherung von Schwangeren wegen strafbarer Abtreibung

Im Jahr 1990 hatte die Landesbeauftragte für den Datenschutz in Baden-Württemberg bei Prüfungen mehrerer Polizeidirektionen festgestellt, daß in der Personenauskunftsdatei (PAD), die mit dem bayerischen KAN vergleichbar ist, Personen wegen verbotener Abtreibung nach § 218 Abs. 1 i.V.m. Abs. 3 StGB unter Verstoß gegen Datenschutzbestimmungen erfaßt waren. Die Landesbeauftragte hatte die Speicherungen beanstandet und auf die **generelle Problematik** der Speicherung von schwangeren Frauen, die in strafbarer Weise abgetrieben haben, hingewiesen.

Im Verlauf der einsetzenden Diskussion über das Pro und Contra solcher Speicherungen hat das Innenministerium seine bisherige Auffassung aufgegeben und die Speicherung von Frauen, die eine strafbare Abtreibung vorgenommen haben, als polizeitaktisch sinnlos bezeichnet. Fehlt es aber an der Geeignetheit und Erforderlichkeit der Speicherung zur Erfüllung polizeilicher Aufgaben, so ist die Speicherung unzulässig. Ich habe deshalb darauf gedrängt, daß die Polizei die von ihr selbst für unzulässig gehaltenen Speicherungen im KAN unverzüglich löscht. Das Innenministerium hat daraufhin die Löschung aller Straftaten nach § 218 Abs. 1 i.V.m. Abs. 3 StGB im KAN und in der Vorgangsverwaltung sowie die Vernichtung der dazugehörenden Kriminalakten angeordnet. Vom Vollzug habe ich mich durch Stichproben überzeugt.

4.14 Bürgereingaben

Ein Schwerpunkt der Bürgereingaben waren wie in den Vorjahren, wenn auch in etwas geringerem Umfang, **Anfragen wegen vermuteter Speicherungen** bei Polizeibehörden aufgrund konkreter Vorfälle.

In den Vorjahren wurden gelegentlich Bürger, die bei einer Polizeidienststelle Auskunft über die zu ihrer Person gespeicherten Daten verlangten, an mich verwiesen. Dies habe ich im Berichtszeitraum nicht mehr festgestellt. Offensichtlich werden nach Einfügung des Auskunftsrechts in Art. 48 PAG von den speichernden Stellen mehr Auskunftsanträge zur Zufriedenheit der Anfragenden beantwortet.

Ein anderer Schwerpunkt der Bürgereingaben betraf die **weitere Aufbewahrung** polizeilicher Unterlagen und die fortbestehende Speicherung in polizeilichen Dateien/Karteien, obwohl die Strafverfahren der Betroffenen eingestellt oder mit einem Freispruch abgeschlossen worden waren. Zur Bedeutung von Verfahrenseinstellungen und Freisprüchen für die weitere Speicherung im KAN habe ich mich bereits im 12. Tätigkeitsbericht geäußert. Nach Art. 38 Abs. 2 Satz 1 PAG kann die Polizei insbesondere personenbezogene Daten, die sie im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen gewonnen hat, die verdächtig sind, eine Straftat begangen zu haben, speichern, verändern oder nutzen, soweit dies zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Entfällt der der Speicherung zugrunde liegende Verdacht, so sind die Daten in der Datei zu löschen und die Kriminalakte zu vernichten, soweit nicht die Voraussetzungen einer Sperrung oder Archivierung vorliegen.

Der Verdacht kann insbesondere entfallen, wenn die Staatsanwaltschaft oder das Gericht feststellen, daß keine Straftat vorliegt oder der Beschuldigte als Täter ausscheidet. Da es sich beim KAN und bei der Kriminalakte um Unterlagen der Polizei handelt, ist für die Frage, ob der Verdacht entfallen ist, nicht die Einschätzung der Justiz, sondern letztlich die der **Polizei maßgeblich**, zumal die Unterlagen der Gefahrenabwehr und Kriminalitätsbekämpfung durch die Polizei dienen.

Leider fehlt in polizeilichen Akten in den meisten Fällen die Begründung bei Verfahrenseinstellungen nach § 170 Abs. 2 StPO. Bürgereingaben sind deshalb nicht immer kurzfristig zu beantworten, weil die Polizei zunächst die erforderlichen Informationen bei der Staatsanwaltschaft anfordern und bewerten muß. Wie wichtig die Kenntnis vom Verfahrensausgang ist, zeigt eine Reihe von Fällen, in denen die Polizei nach Prüfung der Einstellung und deren Begründung personenbezogene Daten löscht, weil festgestellt wird, daß der ursprünglich angenommene Tatverdacht, der zur Anzeige bei der Staatsanwaltschaft geführt hatte, entfallen ist.

Einige Petenten wollten nach vergeblichen Auskunftsersuchen bei der Polizei von mir erfahren, welche Informationen die zuständige Polizeidienststelle über sie speichert. Die Anfragen betrafen somit neben den Speicherungen im KAN auch solche in der Vorgangsverwaltung sowie in anderen von der Polizei geführten Dateien und Karteien. In diesen Fällen hat die Polizei die Auskunft verweigert, weil eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung, insbesondere eine Ausforschung der Polizei zu besorgen war (Art. 48 Abs. 2 PAG). Meine Überprüfung hat ergeben, daß zu Beanstandungen kein Anlaß bestand.

Bürger wenden sich nicht nur an mich mit der Bitte um **generelle Auskunft** über die zu ihrer Person bei der bayer. Polizei gespeicherten Daten, sondern auch mit dem Wunsch nach Überprüfung **konkreter polizeilicher Vorgänge**. So hatte sich im Vorjahr eine Petentin an mich gewandt und darum gebeten, nachzuprüfen, ob zu ihrer Person aufgenommene erkennungsdienstliche Unterlagen — wie vom Landeskriminalamt zugesagt — tatsächlich vernichtet worden sind. Meine Nachprüfung hatte ergeben, daß die ED-Unterlagen tatsächlich vernichtet waren. Dies habe ich der Betroffenen mitgeteilt.

Mit dem Antrag an den Landesbeauftragten, die Vernichtung der erkennungsdienstlichen Unterlagen zu überprüfen, wollte sich die Petentin nur vergewissern, ob das Landeskriminalamt sich an seine Zusage gehalten hat. Die Antragstellerin hat damit von mir keine umfassende Prüfung verlangt, ob sie in den verschiedenen anderen Dateien der Polizei gespeichert ist. Aus meiner Bestätigung, daß die erkennungsdienstlichen Unterlagen vernichtet sind, kann auch nicht der Schluß gezogen werden, daß man auch sonst in den verschiedenen Dateien und Akten der Polizei nicht gespeichert ist. Tatsächlich bestanden im vorliegenden Fall wegen des Vorfalls, der zur erkennungsdienstlichen Behandlung geführt hatte, noch eine Kriminalakte zur Person der Betroffenen und eine entsprechende Speicherung im KAN.

Um künftigen Mißverständnissen bei Bürgern vorzubeugen, die nur die Überprüfung eines ganz bestimmten Verhaltens der Polizei wünschen, werde ich nach der Erfahrung dieses Falles in Antwortschreiben darauf hinweisen, daß mit der Überprüfung des vom Petenten bezeichneten Verhaltens der Polizei keine Generalauskunft über Speicherungen des Betroffenen in den Dateien und Akten aller bayerischen Polizeidienststellen verbunden ist.

Im vorliegenden Fall hatte die Petentin bei der Polizeidienststelle nach kriminalpolizeilichen Ermittlungen, ED-Behandlung und Verfahrenseinstellung durch die Staatsanwaltschaft nach § 170 Abs. 2 StPO die Vernichtung der ED-Unterlagen gefordert. Nach der erkennbaren Interessenlage der Petentin hätte die Polizeidienststelle freilich auch prüfen müssen, ob und ggf. in welchem Umfang die Vernichtung der **sonstigen** in diesem Zusammenhang angefertigten polizeilichen Unterlagen geboten gewesen wäre. Diese Prüfung ist unterblieben. Das habe ich beanstandet und die Dienststelle aufgefordert, für die Zukunft die Durchführung der erforderlichen Prüfung sicherzustellen.

Das Landeskriminalamt, das für Entscheidungen über Anträge auf Vernichtung von erkennungsdienstlichen Unterlagen und KAN-Löschungen zuständig ist, hat diese Prüfung ebenfalls unterlassen und sich in seinem Antwortschreiben an die Petentin allein mit der Vernichtung der erkennungsdienstlichen Unterlagen befaßt. Dadurch ist bei ihr der Eindruck entstanden, daß damit alle Speicherungen im Zusammenhang mit dem betreffenden Vorgang gelöscht sind. Diese Sachbehandlung habe ich ebenfalls beanstandet.

Das Innenministerium habe ich gebeten, bei der Behandlung solcher Fälle folgende Grundsätze zu berücksichtigen:

1. Eingabeschreiben von Bürgern, die in der Regel mit der äußerst komplexen Datenverarbeitung der Polizei nicht vertraut sind, sind aus der Interessenlage des Petenten heraus auszulegen. Die Polizei darf nicht eng am Wortlaut des Antrags festhalten.

2. Bezeichnet ein Bürger in seinem Antrag auf Vernichtung von Unterlagen nur **Teile** der von der Dienststelle angefertigten Unterlagen, ergibt aber die Auslegung des Antrags, daß er die Löschung **aller** in diesem Zusammenhang angefertigten Unterlagen wünscht, dann ist die Vernichtung aller dieser Unterlagen zu prüfen. Können nicht alle Unterlagen vernichtet werden, so ist er hierauf im Antwortschreiben ausdrücklich hinzuweisen.

3. Im Falle der antragsgemäßen Vernichtung von erkennungsdienstlichen Unterlagen wegen **fehlenden Tatverdachts** ist auch die den Vorgang betreffende Kriminalakte zu vernichten und die entsprechende Speicherung im KAN zu löschen. Gleiches gilt für Speicherungen in anderen Unterlagen und Dateien, die der polizeilichen Aufgabenerfüllung dienen. Für die Vorgangsverwaltung ist sicherzustellen, daß die zu diesem Vorgang gespeicherten Daten für Zwecke der Verbrechensbekämpfung nicht mehr genutzt werden können.

4. In den Antwortschreiben kann die Polizei allerdings die Gesichtspunkte berücksichtigen, die nach Art. 48 Abs. 2 PAG zur Verweigerung der Auskunft berechtigen.

5. Verfassungsschutz

5.1 Vorbemerkung

Zu den Kontrollinstanzen, die den Verfassungsschutz zu überwachen haben, gehört neben dem Innenministerium, dem Rechtsausschuß des Landtags, der G 10-Kommission und der Parlamentarischen Kontrollkommission auch der Landesbeauftragte für den Datenschutz. Seine Rolle besteht hauptsächlich darin, die Dateien und Karteien des Landesamts für Verfassungsschutz, somit die Erhebung und Verarbeitung der Daten über Bürger zu kontrollieren. Da die Tätigkeit des LfV im wesentlichen aus Informationsbeschaffung, -sammlung und -auswertung besteht, umfaßt meine Kontrollkompetenz somit den größten Teil der Tätigkeit des Landesamts für Verfassungsschutz. Für einen **weiteren Kontrolleur** besteht aus meiner Sicht kein Bedürfnis.

Schwerpunkte meiner Tätigkeit im Berichtszeitraum waren eine mehrtägige allgemeine Prüfung, Kontrollen aufgrund von Bürgereingaben sowie die Beratung des LfV insbesondere bei der Anwendung des neuen Bayer. Verfassungsschutzgesetzes. Im vorliegenden Bericht findet diese Tätigkeit wie in den Vorjahren nur insoweit ihren Niederschlag, als die Erfüllung der Aufgaben des LfV dadurch nicht beeinträchtigt wird.

5.2 Existenzberechtigung des Verfassungsschutzes

Nach den Umwälzungen im Osten wurden in der Öffentlichkeit verstärkt Zweifel an der Existenzberechtigung des Verfassungsschutzes geäußert. Wenn diese Institution zum Schutz unserer freiheitlichen demokratischen Grundordnung, für den Bestand oder die Sicherheit des Bundes oder eines deutschen Landes sowie zur Abwehr sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten nicht mehr erforderlich wäre, dann wäre es auch unzulässig, weiterhin mit nachrichtendienstlichen Mitteln Informationen über Bürger zu beschaffen, die gewonnenen Daten auszuwerten und für den Schutz der Verfassung und des Staates zu nutzen. Doch davon abgesehen, daß sich die Situation allenfalls gewandelt hat, jedoch auch weiterhin generell mit verfassungs- und staatsfeindlichen Bestrebungen zu rechnen ist, ist die Diskussion um die Existenzberechtigung des Verfassungsschutzes nach dem verstärkten Auftreten militanter Rechtsextremisten, insbesondere in den neuen Bundesländern, rasch verstummt.

5.3 Behinderung des Verfassungsschutzes durch den Datenschutz

Nach dem Attentat auf Treuhandchef C. Rohwedder wurde wegen seit Jahren ausbleibender Erfolge bei der Terroristenfahndung in der Öffentlichkeit auch die Frage erörtert, ob der Datenschutz — Gesetze ebenso wie behördliche Kontrolle — die Sicherheitsbehörden und damit auch den Verfassungsschutz an effektiver Aufklärung behindere. In einem Gespräch mit dem Innenministerium und dem LfV bestand Einvernehmen, daß verfassungsrechtlich gebotener Datenschutz Erschwernisse bei der Arbeit der Sicherheitsbehörden mit sich bringe, diese Beschränkungen aber dem Rechtsstaat immanent und deshalb außer jeder Diskussion stünden. Es herrschte aber auch Einvernehmen darüber, daß nicht alle Hindernisse, die im Namen des Datenschutzes aufgerichtet würden, von der rechtsstaatlichen Ordnung gefordert seien.

Innenministerium und LfV zeigten Verständnis für meine Auffassung, daß **Kontrollhäufigkeit** und **Kontrolldichte** angesichts besonders sensibler Daten, die eine regelmäßig im Vorfeld konkreter Gefahrenlagen und verdeckt operierende Behörde beschaffe und auswerte, nicht zurückgenommen werden könnten. Ich beabsichtige allerdings nicht, mich an **gemeinsamen Kontrollen** anderer Datenschutzbeauftragter zu beteiligen, weil hierdurch nur unnötige Verunsicherung in den Verfassungsschutz hineingetragen wird, ohne Gewinn für den Datenschutz. Andererseits erhob ich keine Bedenken gegen die Absicht des LfV, die Erfahrungen der letzten Jahre in der Terroristenfahndung bei der Führung der LfV-Dateien zu berücksichtigen.

5.4 Zusammenfassende Feststellung

Als Gesamtergebnis meiner Kontrolle im Berichtszeitraum kann ich feststellen, daß das LfV dem Datenschutz einen sehr hohen Stellenwert einräumt. Die Anpassung der gespeicherten Datei- und Karteibestände an die neue Rechtslage sowie die forcierte Umstellung von Karteispeicherung auf automatisierte Datenverarbeitung haben zu einer starken Reduzierung der Speicherungen geführt. Zu diesem grundsätzlich erfreulichen Ergebnis hat nach Auffassung des LfV freilich auch der starke Rückgang der Meldungen von Behörden, insbesondere der Polizei, an das LfV beigetragen.

5.5 Generelle Prüfung 1991

Im Berichtszeitraum habe ich beim Landesamt wieder eine mehrtägige Prüfung verschiedener Dateien und Karteien vorgenommen.

Schwerpunkte waren insbesondere Speicherungen

- im Nachrichtendienstlichen Informationssystem NADIS der Verfassungsschutzbehörden
- in Dateien und Karteien der Bereiche „Terrorismus links", „Terrorismus rechts", „Extremismus links", „Extremismus rechts" und „Ausländerextremismus".

Wesentliche Verstöße gegen datenschutzrechtliche Bestimmungen habe ich dabei **nicht festgestellt**.

Bei den Überprüfungen der NADIS-Speicherungen wurden die dazugehörenden Karteikarten und Akten zugezogen und im Einzelfall von den Vertretern des LfV erläutert.

Bei den ausgewählten Stichproben waren Personen gespeichert, die wegen Teilnahme an „Autonomen-Treffen" oder als derzeit oder ehemals verantwortliche Mitglieder von Parteien oder Gruppierungen, die der Beobachtung unterliegen, zu dem Personenkreis gehörten, die in NADIS erfaßt werden dürfen.

Die im Vorjahr vom LfV angekündigte Überprüfung der korrekten Vergabe des **Erkenntnisdatums**, das den Zeitpunkt des letzten für die Speicherung in NADIS relevanten Ereignisses angeben soll, wurde durchgeführt. Bei allen meinen Stichproben war das Erkenntnisdatum, an das die Berechnung der Speicherungsdauer anknüpft, zutreffend festgelegt.

Die Kartei „Terrorismus links", die Vorfelderkenntnisse im linksterroristischen Bereich enthält, ist in den letzten Jahren als Folge rückläufiger Meldungen der Polizei und der kurzen Löschungsfristen sowie interner Relevanzprüfungen ganz erheblich zusammengeschmolzen. Stichproben ergaben keinen Anlaß zur Beanstandung. Gleiches galt für die Karteien „Extremismus links".

5.6 Bürgereingaben

Im Berichtsjahr gingen die Bürgereingaben gegenüber den Vorjahren etwas zurück. Diese Entwicklung erklärt sich zum Teil daraus, daß die Bürger nach Maßgabe des Art. 11 BayVSG nunmehr unmittelbar beim Landesamt für Verfassungsschutz (LfV) Auskunft über die dort zu ihrer Person gespeicherten Daten verlangen können. Erhält der Bürger die Auskunft, daß keine Speicherungen über ihn bestehen, wird er häufig von einer Anfrage beim Landesbeauftragten absehen.

Im Berichtszeitraum hat sich kein Bürger mit der Bitte um Nachprüfung einer ihn betreffenden **Sicherheitsüberprüfung** an mich gewandt. Die mit dem Staatsministerium des Innern vereinbarte Information der zu überprüfenden Personen über den Ablauf einer Überprüfung sowie der mit dem Inkrafttreten des Bayer. Verfassungsschutzgesetzes bestehende Anspruch auf Auskunft über die Daten des LfV, die es im Rahmen der Sicherheitsüberprüfung übermittelt hat, haben offenbar zur Beruhigung der Betroffenen beigetragen.

Einzelne Eingaben betrafen **vermutete Sicherheitsüberprüfungen**. Die Vermutungen basierten auf bestimmten Ereignissen, von denen der Betroffene annahm, daß sie ihre Ursache in Speicherungen beim LfV haben. Wird der Petent beispielsweise wiederholt nach Bewerbungen bei Firmen, die Sicherheitsüberprüfungen durchführen, nicht berücksichtigt, dann vermutet er, das LfV habe im Rahmen einer Sicherheitsüberprüfung Sicherheitsbedenken geäußert. Alle meine Prüfungen in diesem Zusammenhang haben aber ergeben, daß keine Sicherheitsüberprüfungen durchgeführt worden sind, so daß die Ablehnung der Bewerbungen auf andere Gründe zurückzuführen war. Häufig ist auch nicht bekannt, daß das LfV nur dann an einer Sicherheitsüberprüfung mitwirken darf, wenn der Betroffene von der Durchführung der Überprüfung Kenntnis hat. Bei der Überprüfung in der Privatwirtschaft ist sogar das schriftliche Einverständnis des Betroffenen Voraussetzung für ein Tätigwerden des LfV. Hat er also kein Einverständnis für die Überprüfung gegeben, kann er davon ausgehen, daß eine Auskunft des LfV nicht vorlag. Der Bewerber um einen Arbeitsplatz **weiß** demnach, ob eine Sicherheitsüberprüfung eingeleitet worden ist oder nicht.

Soweit ich bei der Überprüfung von Eingaben Speicherungen über die Petenten festgestellt habe, lagen in allen überprüften Fällen die gesetzlichen Voraussetzungen für die Erhebung und Speicherung vor.

Problematisch sind **Teilauskünfte**, wenn das LfV über eine bestimmte Speicherung Auskunft erteilt, aber aus den Gründen des Art. 11 Abs. 3 BayVSG nicht zum Ausdruck bringen will, daß es weitere Informationen besitzt. Damit in einem solchen Fall aus dem nach Art. 11 Abs. 4 BayVSG vorgeschriebenen Hinweis auf den Landesbeauftragten nicht auf weitere Speicherungen geschlossen werden kann, bleibt letztlich nur die Möglichkeit, die Auskunft insgesamt zu verweigern.

5.7 Interne Arbeitsanweisungen

Das Bayer. Verfassungsschutzgesetz stellt die gesetzliche Grundlage für die Tätigkeit des Landesamts für Verfassungsschutz (LfV) dar. Das Gesetz verwendet jedoch zwangsläufig viele unbestimmte Rechtsbegriffe und Generalklauseln, die nur den Handlungsrahmen des LfV mit der verfassungsrechtlich gebotenen Genauigkeit festlegen. Das Gesetz soll und kann aber weder sein eigener Kommentar sein noch interne Richtlinien ersetzen. Schon gar nicht kann es die rechtliche Einordnung von politischen Gruppierungen, wie sie in der Wirklichkeit auftreten, vornehmen. Das Gesetz soll nur das Notwendige regeln. Für die tägliche Arbeit der Datenerhebung und -verarbeitung bedarf es vielmehr entsprechend den spezifischen Aufgaben und praktischen Notwendigkeiten konkreter, die unbestimmten Rechtsbegriffe und Generalklauseln ausfüllender Arbeitsanweisungen.

Die Arbeitsanweisungen an die einzelnen Abteilungen zur Errichtung, Führung und Nutzung von Dateien und Karteien sind 1991 überarbeitet, soweit noch nicht vorhanden, erstellt worden. Ich hatte Gelegenheit, vor Erlaß dieser internen Richtlinien zu den Entwürfen schriftlich und in Besprechungen mit dem Innenministerium und dem LfV Stellung zu nehmen.

Meine Anregungen sind bei der Erstellung der Arbeitsanweisungen berücksichtigt worden.

5.8 Datei „Karteiüberwachung"

Nach Art. 8 Abs. 2 BayVSG hat das LfV bei jeder Einzelfallbearbeitung und nach festgesetzten Fristen zu entscheiden, ob die Speicherungen für die Erfüllung seiner gesetzlich festgelegten Aufgaben noch erforderlich sind. **Die Einhaltung der in den Karteikarten festgesetzten Fristen** wird seit Anfang des Jahres 1991 durch ein **automatisiertes Überwachungsverfahren** unterstützt. Die Sachbearbeiter erhalten bei Ablauf der Frist mit Hilfe der Datei erstellte Wiedervorlagelisten, die sie an die Prüfung der aufgeführten Vorgänge erinnern. Nach einer ersten Besichtigung meine ich, daß das Verfahren die Einhaltung der gesetzlichen Vorgaben wesentlich erleichtert und damit zu einer Verbesserung des Datenschutzes beiträgt.

5.9 Überwachung der Partei des demokratischen Sozialismus (PDS) in Bayern

Da sich der Bund und die Länder nicht auf ein gemeinsames Vorgehen gegenüber der PDS verständigen konnten, hat der Bayer. Staatsminister des Innern veranlaßt, daß die PDS — Landesverband Bayern durch das LfV mit nachrichtendienstlichen Mitteln beobachtet wird. Die Voraussetzungen des Bayer. Verfassungsschutzgesetzes (BayVSG) hierfür liegen vor. Das LfV hat nach Art. 3 BayVSG u.a. die Aufgabe, Bestrebungen im Geltungsbereich des Grundgesetzes, die gegen die freiheitliche demokratische Grundordnung gerichtet sind, zu beobachten. Nachrichtendienstliche Mittel dürfen angewendet werden, wenn tatsächliche Anhaltspunkte für solche Bestrebungen vorliegen (Art. 6 Abs. 1 BayVSG).

Solche tatsächlichen Anhaltspunkte für Bestrebungen der PDS gegen die freiheitliche demokratische Grundordnung ergeben sich nach den Erkenntnissen des Staatsministeriums des Innern, die mir zugänglich gemacht wurden, insbesondere aus

- der programmatischen Berufung auf die kommunistische Tradition einschließlich Lenin,
- der vom PDS-Vorstand satzungsgemäß akzeptierten starken „kommunistischen Plattform" innerhalb der Partei,
- der weitgehend personellen Identität der Mitgliedschaft der PDS mit derjenigen der alten SED,
- der Zusammenarbeit mit anderen linksextremistischen Gruppierungen.

Zur Rolle von „Plattformen" bestimmt das PDS-Statut, daß innerhalb der Partei Plattformen gebildet werden, die die programmatische Arbeit der Partei und ihre Strukturen unterstützen. Diese Plattformen seien berechtigt, die Einrichtungen und Arbeitsmittel der Partei zu nutzen. Am 23. November 1990 veröffentlichte der PDS-Pressedienst einen überarbeiteten Entwurf der „Thesen für eine Plattform der KommunistInnen in der PDS". Darin heißt es u.a., der Klassenkampf bleibe das elementare Wesen der sozialen, politischen und ideologischen Auseinandersetzungen. Da der „bürgerliche Staat" letztlich ein Machtinstrument der herrschenden Klasse sei, blieben Versuche, ihn über seine parlamentarischen Organe und „Gestaltungspolitik" aufzuheben, illusionär. Es gehe darum, ihn, also den parlamentarischen demokratischen Staat, revolutionär-demokratisch zu überwinden.

Ein weiterer entscheidender Grund für die Einstufung der PDS als verfassungsfeindliche Gruppierung ist nach Darstellung des Innenministeriums der Personalkörper der PDS, der zu 99 % aus Mitgliedern der ehemaligen SED besteht. Die PDS ist die umbenannte SED, in der ganz überwiegend ehemalige SED-Leute und Funktionäre tätig sind.

Hiergegen ist entgegen der Auffassung anderer Datenschutzbeauftragter neben Anhaltspunkten für den Verdacht verfassungsfeindlicher Bestrebungen nicht weitere Voraussetzung für die Beobachtung der PDS durch den Verfassungsschutz, daß diese Partei die freiheitliche demokratische Grundordnung bereits tatsächlich gefährde. Nach dieser abzulehnenden Auffassung darf die Beobachtung durch das Schutzorgan erst einsetzen, wenn die Ablehnung der freiheitlichen demokratischen Grundordnung eine Gefährdung darstellt.

Dieses zusätzliche Tatbestandsmerkmal der tatsächlichen Gefährdung steht weder im Bayerischen Verfassungsschutzgesetz noch im Bundesverfassungsschutzgesetz, noch ergibt sich diese Voraussetzung aus dem Wort „Bestrebungen" noch aus dem ungeschriebenen Verfassungsgrundsatz der Verhältnismäßigkeit.

Wer schon für die Beobachtung einer verfassungsfeindlichen Gruppierung das Vorliegen einer tatsächlichen Gefährdung der freiheitlichen demokratischen Grundordnung fordert, der verwechselt den Verfassungsschutz mit der Polizei. Ferner kann die tatsächliche Gefährdung der freiheitlichen demokratischen Grundordnung erst bei der Frage, ob eine als verfassungswidrig erkannte Partei nach Art. 21 Grundgesetz **verboten** werden soll und hierzu der Antrag beim Bundesverfassungsgericht zu stellen ist, relevant sein. Der Verfassungsschutz kann aber nicht erst mit der Beobachtung anfangen, wenn die Partei schon verboten werden müßte. Woher soll die antragstellende Regierung denn die Informationen für den Verbotsantrag beziehen? Aus der Zeitung? Ohne vorherige Beobachtung durch den Verfassungsschutz wäre ein Parteienverbot in der Regel aussichtslos. Im übrigen: Aus welchen Quellen soll eine Regierung über die tatsächliche Gefährdung einer konspirativ tätigen Gruppierung erfahren, wenn nicht vom Verfassungsschutz? Schließlich: Wenn der Verfassungsschutz mit dem Beobachten erst anfangen dürfte, wenn die freiheitliche demokratische Grundordnung bereits tat-

sächlich gefährdet ist, dann käme die Beobachtung zu spät, der Verfassungsschutz hätte seinen Auftrag verfehlt.

Bis jetzt ist nicht bekannt geworden, daß die PDS gegen die Beobachtung durch das LfV gerichtliche Schritte unternommen habe.

5.10 Kontrolle der Anwendungen nachrichtendienstlicher Mittel

Bei **Anwendung nachrichtendienstlicher Mittel** durch das Landesamt für Verfassungsschutz fordert das BayVSG keine gesonderte Dokumentation oder Aufzeichnung dieser Einsätze. Eine gesetzliche Aufzeichnungs**pflicht** hätte meine Kontrolltätigkeit erleichtert. Die unverzichtbare Kontrolle beim Einsatz bestimmter nachrichtendienstlicher Mittel durch den Datenschutzbeauftragten kann somit nur durch **mehr Kontrollaufwand** bei der Überprüfung der Speicherung einschließlich der vorausgehenden Datenerhebungen erreicht werden.

6. Justiz

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

Der Bundesrat hat den von ihm in der vorigen Legislaturperiode verabschiedeten Entwurf eines OrgKG überarbeitet und am 26. April 1991 neu beschlossen.

Der Gesetzentwurf ist vor dem Hintergrund einer bedrückenden Kriminalitätsentwicklung, insbesondere im Bereich der Rauschgiftkriminalität und anderer Kriminalitätserscheinungen, z.B. auf dem Gebiet der Geldfälschung, der Verschiebung hochwertiger Güter oder der Milieukriminalität im Umfeld der Prostitution zu sehen. Die Entwicklung auf diesem Gebiet ist nicht nur durch einen alarmierenden Anstieg der Straftaten, sondern auch durch eine qualitative Veränderung hin zur organisierten Begehungsweise gekennzeichnet. Die Verbrechen zeugen davon, daß die Straftäter — meist international verflochten — persönliche und geschäftliche Verbindungen mit großer krimineller Energie und Kapitalkraft nutzen, um hohe illegale Gewinne zu erzielen. Konspirative Vorbereitung und Durchführung der Straftaten erschweren die Verbrechensbekämpfung. Deren Erfolge hängen davon ab, in welchem Umfang es gelingt, die Organisatoren und Drahtzieher der Begehung der Straftaten zu überführen.

Gerade die Rauschgiftkriminalität hat in den letzten Jahren weltweit in bedrohlicher Weise zugenommen. Auch in der Bundesrepublik Deutschland ist die Zahl der Rauschgiftdelikte drastisch gestiegen, der Drogenmißbrauch hat ein bisher nicht bekanntes Ausmaß angenommen. Im vergangenen Jahr hat die Polizei in den alten Bundesländern rund 1.500 Drogentote registriert, 500 mehr als im Jahr zuvor. Für das Jahr 1991 muß mit etwa 2.000 Drogentoten gerechnet werden. Die durch den illegalen Betäubungsmittelhandel erwirtschafteten Gelder fließen nicht selten in andere Bereiche besonders gewinnträchtiger Kriminalität wie etwa Geld- und Scheckfälschung, Zuhälterringe, Betrieb illegaler Spielkasinos.

Aber auch in anderen Kriminalitätsbereichen, etwa dem bandenmäßigen Diebstahl und Einbruchsdiebstahl, der Verschiebung hochwertiger Kraftfahrzeuge in das Ausland, dem illegalen Waffenhandel und der Erpressung von Schutzgeld, treten in verstärktem Maß kriminelle Organisationen in Erscheinung. Mit herkömmlichen Ermittlungsmethoden lassen sich meist nur die Straftaten von Randfiguren aufklären, die keinen Einblick in Aufbau und Zusammensetzung der Gesamtorganisation haben. Für die Überführung der „Drahtzieher" organisierter Kriminalität fehlt den Strafverfolgungsbehörden derzeit ein ausreichendes gesetzliches Instrumentarium.

Der Gesetzentwurf regelt deshalb Ermittlungsmethoden, die es ermöglichen sollen, über die Peripherie der kriminellen Organisation hinaus in deren Kernbereich einzudringen, ihre Strukturen zu erkennen und zu zerschlagen und die Hauptverantwortlichen, die Organisatoren, Finanziers und im Hintergrund agierenden Straftäter zu überführen.

Außerdem ist es — acht Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts — dringend geboten, die Datenerhebung und -verarbeitung der Strafverfolgungsorgane, insbesondere die neuen Fahndungsmethoden, auf eine tragfähige gesetzliche Grundlage zu stellen und auf diesem sensiblen Gebiet für Rechtsklarheit zu sorgen.

Aus der Sicht des Datenschutzes sind wegen des Eingriffs in das Recht auf informationelle Selbstbestimmung von besonderem Interesse:
- der Einsatz **verdeckter Ermittler** (Polizeibeamte unter einer Legende),
- der **verdeckte Einsatz technischer Mittel** (Lichtbilder, Bildaufzeichnungen, besondere Sichthilfen und akustische Überwachungsgeräte),
- die **Rasterfahndung**, der **Datenabgleich** und die polizeiliche **Beobachtung**,
- die Erweiterung der **Telefonüberwachung** auf Bandenkriminalität und zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben und Freiheit einer Person.

Die Mehrzahl der Datenschutzbeauftragten des Bundes und der Länder hat vor schwerwiegenden Eingriffen in die Bürgerrechte, so wie sie im Gesetzentwurf vorgesehen seien, gewarnt. Diese Kritik halte ich nicht für verantwortbar und habe dies in einer ei-

genen Presseerklärung vom 26.6.1991 deutlich gemacht:

- Die Entschließung wendet sich gegen beabsichtigte Regelungen, ohne die Folgen für eine wirksame Kriminalitätsbekämpfung in Betracht zu ziehen. Durch die geforderten Einschränkungen der bisherigen Praxis bei Bild- und Filmaufnahmen, in die auch Kontaktpersonen einbezogen sind, würde künftig Verbrechern das Untertauchen und Verschwinden, das Verwischen von Spuren und die Sicherung ihrer Beute wesentlich erleichtert. Bei schweren Straftaten müssen als ultima ratio auch technische Mittel wie Richtmikrophone verwendet werden dürfen, wenn sonst die Aufklärung nicht möglich ist.

- In anderen Teilen erweckt die Entschließung ohne Anhaltspunkte im Gesetzentwurf den unrichtigen Eindruck, als würden ohne Not zusätzliche Eingriffe in Grundrechte erlaubt. Die akute Bedrohung durch die organisierte Kriminalität, insbesondere die Rauschgift- und terroristische Gewaltkriminalität, wird nicht berücksichtigt.

- Eilkompetenzen für die Staatsanwaltschaft und ihre Hilfsbeamten werden ohne Rücksicht auf die Folgen der Verzögerung für die geordnete Strafverfolgung abgelehnt, während solche Kompetenzen nach geltendem Recht für weit gravierendere Eingriffe unbestritten sind. Die Verwischung von Spuren und die Sicherung der Beute werden ohne Not in Kauf genommen.

- Auf dem Gebiet der Schwerkriminalität, insbesondere der organisierten Kriminalität, wird die vorbeugende Straftatenbekämpfung durch die Polizei, würde man der Entschließung der Datenschutzbeauftragten folgen, dadurch wesentlich erschwert, daß die bisherige Nutzung von rechtmäßig gewonnenen Informationen aus dem Einsatz nichtoffener Ermittlungsmethoden für die Zukunft in Frage gestellt wird. Es wird verlangt, daß die Polizei ihr Wissen zur Verhütung von Straftaten nicht mehr im bisher zulässigen Umfang nutzen darf.

Nach meiner Überzeugung, die auch vom Datenschutzbeirat geteilt wird, bemüht sich der Gesetzentwurf, dem die Bundesregierung mit einigen Änderungen zugestimmt hat, mit Erfolg darum, die Balance zwischen den Erfordernissen einer wirksamen Verbrechensbekämpfung und dem Schutz des Einzelnen vor staatlichen Eingriffen zu wahren. Die Ablehnung des Entwurfs würde nur vordergründig die Freiheitsrechte der Bürger schützen, in Wirklichkeit aber der Freiheit und dem Schutz aller Bürger schaden. Datenschutz darf nicht zum Täterschutz werden.

Die grundsätzliche Zustimmung zum Gesetzentwurf als tragfähige Grundlage zu einer verbesserten Bekämpfung der organisierten Kriminalität schließt jedoch nicht aus, daß in datenschutzrechtlicher Hinsicht in Detailfragen weitere Verbesserungen im Gesetzgebungsverfahren angestrebt werden sollten, wie etwa

- in Eilfällen zumindest eine **nachträgliche Kontrolle** des Einsatzes besonderer Ermittlungsmethoden durch Richter oder Datenschutzbeauftragte,

- eine **Präzisierung** des Begriffs „Straftaten von erheblicher Bedeutung" durch Aufnahme eines Beispielkataloges, wie in einigen Länderpolizeigesetzen (Art. 30 Abs. 5 PAG),

- eine **Information** des Datenschutzbeauftragten über Rasterfahndungen,

- die nachträgliche Unterrichtung der Betroffenen vom Einsatz besonderer Observationsmittel, z.B. Peilsender,

- die Verschärfung der Subsidiaritätsklausel beim Einsatz verdeckter Ermittler; ein solcher Einsatz sollte nur in Betracht kommen, wenn die Aufklärung der Straftat oder die Festnahme des Täters auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Wegen der nur sehr begrenzten Tauglichkeit verdeckter Ermittler im Milieu schwerer organisierter Kriminalität sollte allerdings auch überlegt werden, ob der **Einsatz von technischen Mitteln in Räumen**, begrenzt auf Fälle des Rauschgifthandels und ähnlich schwerer organisierter Kriminalität, unter strikter richterlicher Kontrolle sowie für eine zeitlich begrenzte Erprobung zugelassen werden sollte.

Wenn den deutschen Strafverfolgungsorganen die notwendigen, in Ländern mit rechtsstaatlicher Tradition zugelassenen Aufklärungsmittel vorenthalten werden, wächst die Gefahr, daß Deutschland zum Tummelplatz internationaler Verbrecher wird.

Ähnliche Überlegungen müssen für Einschränkungen des im Grundgesetz verankerten Brief-, Post- und Fernmeldegeheimnisses gelten. Dieses Grundrecht steht unter einfachem Gesetzesvorbehalt (Art. 10 Abs. 2 GG). Wenn die deutschen Sicherheitsbehörden zu Recht befürchten, daß die Aktivitäten der internationalen Drogenmafia in dramatischer Weise zunehmen und die deutsche Wirtschaft von weltweit agierenden Drogenhändlern unterwandert werden könnte, oder wenn die deutschen Sicherheitsbehörden darauf angewiesen sind, daß sie Informationen über die Lieferung von Giftgasfabriken, Nukleartechnik und anderen Kriegswaffen von befreundeten Diensten erhalten, dann ist es höchste Zeit, die Grenzen des Brief-, Post- und Fernmeldegeheimnisses zu überdenken.

6.2 Novellierung des Strafvollzugsgesetzes

Im Strafvollzug werden zahlreiche personenbezogene Daten der Gefangenen erhoben, in Dateien und Akten gespeichert, an andere Stellen übermittelt oder auf sonstige Weise verarbeitet. Die Daten werden erhoben bei dem Gefangenen selbst, aus Unterlagen oder bei anderen Personen oder Stellen. Daten werden aber nicht nur über Gefangene, sondern auch über Personen außerhalb der Justizvollzugsanstalt erhoben, etwa wenn sie in einer für den Strafvollzug bedeutsamen persönlichen oder verwandtschaftlichen Beziehung zu dem Gefangenen stehen oder wenn sie ihn besuchen oder ihm während eines Urlaubs aus der Haft Unterkunft gewähren wollen. Neben der Speicherung personenbezogener Daten in Gefangenenpersonalakten werden solche Daten auch in automatisierten Verfahren zur Lohnabrechnung und Buchführung und in automatisierten Alarm- und Kommunikationssystemen verarbeitet.

Das Strafvollzugsgesetz enthält **kaum gesetzliche Regelungen** zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Strafvollzug. Die bestehenden Verwaltungsvorschriften sind keine ausreichende Grundlage für Eingriffe in das Recht der Gefangenen auf informationelle Selbstbestimmung. Im Hinblick auf das Volkszählungsurteil des Bundesverfassungsgerichts muß **zumindest der Rahmen** für den Umgang mit personenbezogenen Daten im Strafvollzug in einem formellen Gesetz festgelegt werden. Auf diese Notwendigkeit und auf die wichtigsten regelungsbedürftigen Fragen habe ich bereits in mehreren vorangegangenen Tätigkeitsberichten hingewiesen. Der Bundesminister der Justiz hat im Berichtszeitraum einen Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes (Stand 25. März 1991) vorgelegt, der das Strafvollzugsgesetz um die erforderlichen bereichsspezifischen Vorschriften über den Schutz und die Verwendung personenbezogener Daten im Strafvollzug ergänzen soll. Das Bayer. Staatsministerium der Justiz hat mir diesen Entwurf zur Stellungnahme übersandt.

Ich habe mich grundsätzlich positiv zu dem Entwurf geäußert, da er die wesentlichen Fragen der Datenerhebung, Verarbeitung und Nutzung im Strafvollzug unter Berücksichtigung der berechtigten Interessen der davon Betroffenen regelt. Der Entwurf stellt eine tragfähige Grundlage für die weitere Diskussion dar, zu der ich mit weiteren Verbesserungsvorschlägen gegenüber dem Bayer. Staatsministerium der Justiz beigetragen habe. Unter anderem habe ich gefordert, daß

- der Gefangene vor einer Datenübermittlung an nicht-öffentliche Stellen oder Personen **Gelegenheit zur Stellungnahme** erhält.
- auch die berechtigten Interessen des Betroffenen Berücksichtigung finden, soweit beabsichtigt ist, öffentlichen Stellen Akten zu überlassen, weil Auskünfte einen unverhältnismäßig hohen Aufwand erfordern würden,
- die Möglichkeit einer Offenbarung von **medizinischen** Erkenntnissen gegenüber der Anstaltsleitung weiter eingeschränkt wird,
- die vorgesehene **Aufbewahrungsdauer** von Akten mit personenbezogenen Daten von 30 bzw. 50 Jahren überprüft wird.
- die Verarbeitung und Nutzung personenbezogener Daten in nicht anonymisierter Form für wissenschaftliche Zwecke grundsätzlich nur mit Einwilligung des Betroffenen erfolgt.

Weitergehende Forderungen, wonach die Datenerhebung über den Gefangenen, z.B. im Aufnahmeverfahren, bei der ärztlichen Untersuchung oder bei der sog. Behandlungsuntersuchung, in den gesetzlichen Vorschriften bis ins einzelne detailliert geregelt werden sollte, erscheinen mir überzogen. Ich halte es für zulässig, daß auch generalisierende Formulierungen im Interesse der Verständlichkeit, Lesbarkeit und eines vernünftigen Vollzugs verwendet werden, wenn dabei der Grundsatz der Normenklarheit beachtet wird.

6.3 Justizmitteilungsgesetz (JuMiG)

Der Bundesminister der Justiz hat einen weiteren Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) vorgelegt. Das Gesetz soll die erforderliche gesetzliche Grundlage schaffen für die Übermittlung sensibler personenbezogener Daten, die im Justizbereich anfallen. Die Übermittlung innerhalb der Justiz und an andere Stellen findet bisher noch aufgrund von Verwaltungsvorschriften (MiStra und MiZi) statt.

Nach dem Entwurf soll das Justizmitteilungsgesetz nur auf diejenigen von Amts wegen vorzunehmenden Übermittlungen personenbezogener Daten anzuwenden sein, für die bereichsspezifische Datenübermittlungsregelungen fehlen. Der Entwurf enthält gegenüber dem Vorentwurf erfreuliche Verbesserungen:

- Eine Datenübermittlung ist dann zulässig, wenn die Kenntnis der Daten aus der Sicht der übermittelnden Stelle erforderlich **ist** und nicht schon dann, wie noch nach dem Vorentwurf, wenn sie für die Erfüllung der Aufgaben des Empfängers erforderlich sein **kann**.
- Eine Datenübermittlung in Strafsachen vor rechtskräftigem Abschluß oder vor nicht nur vorläufiger Einstellung des Verfahrens ist nur noch dann zulässig, wenn aus der Sicht der übermittelnden Stelle eine besondere Eilbedürftigkeit gegeben ist.
- Übermittlungen in besonders wichtigen oder besonders sensiblen Fällen dürfen nur noch durch

den Richter, den Staatsanwalt oder Amtsanwalt oder durch Beamte des gehobenen Justizdienstes angeordnet werden.

- Bei der Adressierung der Mitteilung ist der übermittelnden Stelle eine gesteigerte Sorgfaltspflicht auferlegt. Sie hat in geeigneten Fällen Vorkehrungen zu treffen, um so weit wie möglich sicherzustellen, daß die Daten unmittelbar den beim Empfänger funktionell zuständigen Bediensteten erreichen.

Der Entwurf enthält jedoch weiterhin einige datenschutzrechtliche Defizite, auf die ich das Bayerische Staatsministerium der Justiz hingewiesen habe:

- Der Entwurf sieht ein zweistufiges Regelungsmodell für die Mitteilungspflichten vor: Danach legt das Gesetz generalklauselartig Fallgruppen fest, in denen eine Datenübermittlung zulässig ist. Die Konkretisierung dieser Fallgruppen sowie die Verpflichtung zur Datenübermittlung bleibt zu erlassenden **Verwaltungsvorschriften** vorbehalten. Vorzuziehen wäre jedoch eine Konkretisierung der Übermittlungstatbestände durch **Rechtsverordnungen** aufgrund einer entsprechenden gesetzlichen Ermächtigung. Damit würden Inhalt und Voraussetzungen der Übermittlungstatbestände durch Rechtsvorschriften festgelegt.

- Es fehlen Regelungen darüber, wie lange die übermittelten Daten beim Empfänger aufbewahrt und verwendet werden dürfen.

- Soweit eine Datenübermittlung im Interesse des Betroffenen erfolgen kann, sollte diese Übermittlung nicht im Ermessen der übermittelnden Behörden stehen, sondern eine Verpflichtung zur Datenübermittlung vorgesehen werden.

Hingegen scheinen mir andere Verbesserungsvorschläge, die diskutiert werden, überzogen:

- Eine generelle Unterrichtung des Betroffenen **vor** der vorgesehenen Übermittlung, damit er Gelegenheit erhält, Bedenken gegen diese vorzubringen, würde zu unnötigen Verzögerungen führen. Die im Entwurf vorgesehene Unterrichtung gleichzeitig mit der Übermittlung halte ich jedenfalls im Regelfall für ausreichend.

- Das Vorliegen des Einverständnisses des Betroffenen als Voraussetzung für eine Mitteilung würde zu einem Erliegen der erforderlichen Justizmitteilungen führen.

6.4 Kontrolle einer Staatsanwaltschaft

Die Prüfung der Datenverarbeitung bei einer Staatsanwaltschaft ergab, daß trotz angespannter Personalsituation infolge der Unterstützung des Aufbaus der Justiz in den neuen Bundesländern auf die Einhaltung datenschutzrechtlicher Bestimmungen **geachtet** wird. Im wesentlichen habe ich folgende Feststellungen getroffen, die in Einzelfällen zu Verbesserungen des Datenschutzes Anlaß geben:

Manuelle zentrale Namenskartei

Bis zur Einführung des automatisiert geführten zentralen Namensregisters Mitte des Jahres 1990 wurden Ermittlungsverfahren in der manuellen zentralen Namenskartei erfaßt. Sie enthält den Namen, das Geburtsdatum des Beschuldigten, den Tatvorwurf und das Aktenzeichen. In einem weiteren Register, das in Buchform geführt wird, finden sich über diese Angaben in der Karteikarte hinaus weitere verfahrensbezogene Daten.

Durch eine stichprobenweise Einsichtnahme in die Kartei habe ich festgestellt, daß eine **Aussonderung** und **Vernichtung** von nicht mehr benötigten Karteikarten des manuellen Namensregisters nur **in unzureichender Form** stattfinden. Die Karteikarten werden nur in unregelmäßigen, mehrjährigen Abständen auf die Notwendigkeit einer Aussonderung hin durchgesehen. Eine Karteikarte wird dann ausgesondert, wenn nach überschlägiger Einschätzung auf der Grundlage von Art und Schwere des zur Last gelegten Delikts, ferner des vermuteten, sich aber nicht aus den Karteikarten ergebenden Verfahrensausgangs und des Alters des Verfahrens davon ausgegangen wird, daß die dazugehörige Akte nicht mehr benötigt wird und möglicherweise bereits vernichtet sein könnte. Bei dieser Vorgehensweise kann es sowohl vorkommen, daß Karteikarten ausgesondert und vernichtet werden, obwohl die dazugehörigen Akten noch aufbewahrt werden, als auch, daß Karteikarten aufbewahrt werden, obwohl die zugrundeliegenden Akten bereits entsprechend den Aufbewahrungsbestimmungen vernichtet worden sind.

Die derzeitige Praxis der Aussonderung von Karteikarten genügt datenschutzrechtlichen Anforderungen nicht. Da Akten jährlich vernichtet werden, müssen auch die dazugehörigen Karteikarten einmal jährlich auf die Notwendigkeit der Aussonderung überprüft werden. Da es sich bei dem Namensregister nur um ein Hilfsmittel zur Auffindung von Verfahrensakten handelt, ist eine Karteikarte zu vernichten, wenn die entsprechenden Verfahrensunterlagen vernichtet werden. Hiervon kann eine Ausnahme allenfalls in den Fällen gemacht werden, in denen auf einer Karteikarte die Daten mehrerer Verfahren eingetragen und noch nicht alle Verfahrensakten vernichtet sind. Auch wenn mit der Existenz einer nicht mehr benötigten Karteikarte im Namensregister regelmäßig keine weiteren für den Betroffenen negativen Folgen verbunden sein mögen, so stellt doch allein die Tatsache der Speicherung personenbezogener Daten bei einer Staatsanwaltschaft einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen dar, der nur im Rahmen des Erforderlichen hingenommen werden kann. Soweit notwendig, sollten die die

Aktenordnung und die Aufbewahrung regelnden Verwaltungsvorschriften den datenschutzrechtlichen Erfordernissen angepaßt werden. Der Meinungsaustausch mit der Justizverwaltung darüber ist noch nicht abgeschlossen.

Automatisierte zentrale Namensdatei

Die automatisierte zentrale Namensdatei ist eine Teilanwendung des bei der Staatsanwaltschaft Landshut erprobten automatisierten Verfahrens „SIJUS-Strafsachen". Seit Mitte des Jahres 1990 werden eingehende Ermittlungsverfahren nur noch in dieser Datei erfaßt. Frühere Eintragungen gegen denselben Beschuldigten im manuellen Namensregister werden in die automatisierte Namensdatei übernommen, die Karteikarten aus dem manuellen Register werden vernichtet. Eine Überprüfung der erfaßten Daten anhand konkreter Vorgänge ergab, daß mehrere bei früheren Prüfungen zentraler Namensregister verschiedener Staatsanwaltschaften kritisierte Unzulänglichkeiten mit dem neuen SIJUS-Verfahren beseitigt sind:

- So wird nun auch die Erledigung eines Ermittlungsverfahrens durch Einstellung mangels hinreichenden Tatverdachts nach § 170 Abs. 2 Strafprozeßordnung in der Datei dokumentiert.

- Der bei Eingang des Verfahrens zugrundeliegende in der Datei gespeicherte Tatvorwurf (Straftatbestand) wird bei wesentlicher Änderung im Laufe des Ermittlungsverfahrens entsprechend dem Tatvorwurf der Anklage neu gefaßt. Da mit dem DV-Verfahren auch die Mitteilungen an das Bundeszentralregister ausgeführt werden, ist in der Datei (nach rechtskräftigem Abschluß des Strafverfahrens) der der Verurteilung zugrundeliegende Tatvorwurf zutreffend erfaßt.

Programmsystem COWISTRA

Die Computerunterstützung in Wirtschaftsstrafsachen (COWISTRA) dient der Erleichterung der Ermittlungen in umfangreichen Strafsachen, insbesondere in Wirtschaftsstrafsachen und in Fällen organisierter Kriminalität. Bei der geprüften Staatsanwaltschaft, einer Schwerpunktstaatsanwaltschaft für Wirtschaftsstrafsachen, wird das automatisierte Verfahren COWISTRA für einige wenige umfangreiche Betrugsverfahren eingesetzt. Zugriff zu dem System haben alle der Wirtschaftsabteilung angehörenden Staatsanwälte, eine Wirtschaftsfachkraft und eine Schreibkraft. Der Zugriffsschutz ist durch die Vergabe einer Benutzerkennung und eines Kennworts ausreichend gewährleistet. Eine stichprobenartige Überprüfung der Speicherungen zu einem konkreten Ermittlungsverfahren ergab keine Anhaltspunkte für eine unzulässige Datenverarbeitung.

Registratur

Eine stichprobenartige Überprüfung der weggelegten Strafakten hat ergeben, daß die für das Jahr 1990 durchzuführende Aktenaussonderung noch nicht vollständig abgeschlossen war. Im Hinblick auf die angespannte Personalsituation der Staatsanwaltschaft habe ich zwar von einer Beanstandung Abstand genommen, aber eine unverzügliche Aktenbereinigung gefordert, die mir auch zugesichert wurde.

Mitteilung des Verfahrensausgangs an die Polizei (Nr. 11 MiStra)

Anhand mehrerer Verfahrensakten habe ich den Vollzug von Nr. 11 MiStra durch die Staatsanwaltschaft geprüft. Nach dieser Vorschrift hat die Staatsanwaltschaft das Aktenzeichen und den Ausgang des Verfahrens mitzuteilen, wenn die Polizei um diese Mitteilung gebeten hat. Dem Verfahrensausgang kann erhebliche Bedeutung für die polizeiliche Datenspeicherung zukommen, je nachdem, ob die Justizentscheidung den der polizeilichen Anzeige zugrundeliegenden Tatverdacht bestätigt oder nicht. Die ordnungsgemäße Mitteilung durch die Staatsanwaltschaft ist somit ein wichtiger Beitrag für die Gewährleistung des Datenschutzes bei der Polizei. Verstöße der Staatsanwaltschaft gegen Nr. 11 MiStra konnte ich nicht feststellen.

Gewährung von Akteneinsicht

Anhand mehrerer Ermittlungsverfahren wurde die Gewährung von Akteneinsicht an private Stellen, insbesondere an Versicherungen, überprüft. Eine Akteneinsicht ist in diesen Fällen nur dann statthaft, wenn und soweit der Antragsteller ein berechtigtes Interesse darlegt. Vor allem bei umfangreichen Verfahren oder bei solchen, die aus mehreren miteinander verbundenen Verfahren mit möglicherweise verschiedenen Geschädigten bestehen, gilt es darauf zu achten, daß die Akteneinsicht nur in diejenigen Teile des Ermittlungsverfahrens gewährt wird, die vom berechtigten Interesse des Antragstellers umfaßt sind. In den von mir überprüften Verfahren entsprach die Gewährung der Akteneinsicht datenschutzrechtlichen Grundsätzen.

6.5. Kontrolle einer Justizvollzugsanstalt

Die Überprüfung des Umgangs mit Daten von Strafgefangenen bei einer Justizvollzugsanstalt ergab, daß die Justizvollzugsanstalt dem Datenschutz einen hohen Stellenwert beimißt. Wesentliche Mängel konnten nicht festgestellt werden.

6.5.1 Manuelle Karteien

Die wesentlichen manuellen Karteien mit Gefangenendaten habe ich stichprobenartig überprüft: die Gefangenenkartei, die Kartei mit besonders gefährlichen Gefangenen, die Besucher- und die Besucherausschlußkartei.

In der **Gefangenenkartei** werden die anwesenden, die vorübergehend abwesenden, die im Vorjahr und die im laufenden Jahr entlassenen Strafgefangenen erfaßt. Diese Kartei gibt einen Überblick über die wichtigsten Daten der Strafgefangenen. Unzulässige, vom Strafvollzugsgesetz nicht gedeckte und für die Erfüllung der Aufgaben der Strafvollstreckung nicht erforderliche Eintragungen konnten nicht festgestellt werden. Die Aufbewahrungszeit der Karteikarten entsprach zutreffend der Aufbewahrungsdauer für die Personalakten gemäß den einschlägigen Aufbewahrungsbestimmungen für den Strafvollzug.

Die **Kartei über besonders gefährliche Gefangene** gibt Hinweise auf eine erhöhte Fluchtgefahr oder eine besondere Gefährlichkeit von Strafgefangenen. Die im Vergleich zu den anderen Gefangenen erhöhte Gefahrenlage ergibt sich z.B. aus einer besonders langen Freiheitsstrafe, aus verübten Gewalttätigkeiten gegenüber dem Anstaltspersonal, aus dem der Haft zugrundeliegenden Straftatbestand, wenn sich daraus Anhaltspunkte für besonders schwere Gewalttätigkeiten entnehmen lassen sowie aus versuchten oder vollendeten Entweichungen. Bei jedem geprüften Fall ließen sich konkrete Anknüpfungstatsachen aus dem Urteil oder aus der Personalakte für das Vorliegen einer erhöhten Gefährlichkeit finden. Über die Vergabe der Vermerke entscheidet ausschließlich der Anstaltsleiter. Datenschutzrechtliche Bedenken gegen die Führung dieser Kartei bestehen nicht.

Die **Besucherkartei** enthält die Namen von Personen, von denen der Gefangene angegeben hat, daß er von ihnen besucht werden möchte. Erscheint eine solche Person, so werden in der Kartei die Personalien, das Datum und die Dauer des Besuchs sowie etwaige Zuwendungen an den Strafgefangenen festgehalten. Die Karteikarte wird bei Entlassung oder Verlegung des Strafgefangenen ausgesondert und zum Personalakt genommen. Gegen die Führung dieser Kartei habe ich keine Bedenken.

In der **Besucherausschlußkartei** befinden sich Personalien von solchen Personen, vorwiegend aus dem terroristischen Bereich, die von Besuchen der Vollzugsanstalten ausgeschlossen sind. Diese Kartei wird nach Angaben der JVA bundeseinheitlich von allen Justizvollzugsanstalten seit den 70er Jahren geführt. Ich habe das Bayer. Staatsministerium der Justiz um Überprüfung gebeten, ob die Voraussetzungen für die weitere Datenspeicherung bei allen erfaßten Personen noch vorliegen.

6.5.2 Zugriff zu Personalakten

Die Personalakten der Strafgefangenen werden in einem versperrten Raum aufbewahrt, der von der Geschäftsstelle aus einsehbar ist. Es kann daher ausgeschlossen werden, daß Gefangene den Raum ohne Aufsicht betreten und in Akten Einsicht nehmen. Allerdings besitzt jeder Vollzugsbeamte der JVA einen Schlüssel zu dem Raum und hat damit Zugriff auf sämtliche Personalakten. Ich habe angeregt zu überprüfen, ob besonders sensible Aktenteile, wie z.B. von Psychologen oder Sozialarbeitern gefertigte Erhebungen über den Gefangenen, Unterlagen über Disziplinarmaßnahmen und soziale Hilfen, in Sonderheften verwahrt und differenzierte Zugriffsberechtigungen für die Bediensteten vergeben werden könnten. Das Ergebnis der Überprüfung steht noch aus.

Die **inhaltliche** Kontrolle mehrerer Personalakten erbrachte keine unzulässigen Eintragungen. Die Personalakten entlassener Strafgefangener werden ordnungsgemäß in einem abgeschlossenen Raum, zu dem nicht jeder Bedienstete Zugang hat, verwahrt. Nach den Aufbewahrungsbestimmungen für den Strafvollzug sind Personalakten entlassener Strafgefangener regelmäßig erst nach 30 Jahren zu vernichten. Zur Zeit der Prüfung erfolgte die Vernichtung von Akten aus dem Jahre 1956. Ich habe auf eine beschleunigte Aktenvernichtung entsprechend den Bestimmungen gedrängt.

6.5.3 Wahrnehmungsbögen

Die Spezialdienste der Justizvollzugsanstalt, wie etwa Sozialarbeiter, Psychologen, Lehrer und Geistliche, führen sogenannte Wahrnehmungsbögen, auf denen der jeweilige Bedienstete Erkenntnisse über den Gefangenen niederlegt. Diese Wahrnehmungsbögen werden den anderen Diensten zugänglich gemacht, um im Interesse einer individuellen Vollzugsbehandlung ein Gesamtbild über den Gefangenen zu erhalten, welches zur gemeinschaftlichen Arbeit an der Resozialisierung erforderlich ist. Gegen diese Datenweitergabe innerhalb der Justizvollzugsanstalt bestehen keine Bedenken, da sie zur Resozialisierung der Gefangenen erforderlich ist. Die Gefangenen sollten jedoch vor den Gesprächen mit den Personen, bei denen sie möglicherweise eine Verpflichtung zur Verschwiegenheit annehmen (insbesondere Psychologen, Anstaltsgeistliche) darauf hingewiesen werden, daß ihre Angaben auf Wahrnehmungsbögen erfaßt und den anderen Diensten zugänglich gemacht werden können.

6.5.4 Automatisierte Verfahren

Automatisierte Verfahren werden in der überprüften JVA vorwiegend für den Bereich der Arbeitsverwaltung und der Abwicklung des Zahlungsverkehrs angewendet. Dateien, die besonders sensible Daten über Strafgefangene enthalten, werden nicht vorgehalten. Die „Datei für die automatisierten Verfahren im Bereich der Bayerischen Justizvollzugsanstalten" (Bereich: allgemein — Arbeitsverwaltung — Zahlstelle) sowie die „Datei für die automatisierte Lohnabrechnung der Gefangenen im Bereich der Bayerischen Justizvollzugsanstalten" (Bereich Arbeitsverwaltung) wurden von mir durch Stichproben über-

prüft. Anhaltspunkte für eine unzulässige Datenverarbeitung habe ich nicht gefunden.

6.6. Datenschutz im gerichtlichen Verfahren

6.6.1 Übersendung psychiatrischer Gutachten an den Prozeßgegner

Im 12. Tätigkeitsbericht hatte ich den Fall einer Klägerin geschildert, die in einem Mietprozeß auf ihre Prozeßfähigkeit hin psychiatrisch untersucht worden war. Sie war zwar mit der Untersuchung einverstanden gewesen, jedoch nicht darauf hingewiesen worden, daß das psychiatrische Gutachten zu den Gerichtsakten genommen und auch dem Prozeßgegner zugänglich gemacht werden würde, um ihm rechtliches Gehör zu gewähren und Gelegenheit zur Stellungnahme zu geben. Die Art der Darstellung des Gutachtens sowie die detaillierte Wiedergabe der von der Probandin freimütig geschilderten persönlichen Verhältnisse, Krankheiten, Schicksalsschläge und Verhaltensweisen führte dazu, daß die Betroffene dem Spott in der Öffentlichkeit ausgesetzt wurde, da der Prozeßgegner den Inhalt des Gutachtens öffentlich verbreitete.

Nach meiner Auffassung sind im Zusammenhang mit der Begutachtung das Persönlichkeitsrecht der betroffenen Klägerin und deren Menschenwürde verletzt worden. Die Anwendung des Prozeßrechts darf nicht dazu führen, daß ein Mensch sich gegenüber einem Gutachter bloßstellen muß mit der Folge, daß seine Offenbarungen gegenüber dem Gutachter mehr oder weniger wörtlich dem Prozeßgegner zur Kenntnis gelangen. Solchen schwerwiegenden Beeinträchtigungen muß unter Beachtung des Grundsatzes des rechtlichen Gehörs durch geeignete Maßnahmen vorgebeugt werden. Anzusetzen ist bereits bei der Erstellung des Gutachtens.

Das Staatsministerium der Justiz, das ich um Stellungnahme gebeten habe, hat auf den verfassungsrechtlich gewährleisteten Anspruch auf rechtliches Gehör hingewiesen und unter diesem Aspekt die Übersendung des Gutachtens durch das Gericht an den Prozeßgegner zur Gewährung des rechtlichen Gehörs für unerläßlich gehalten. Eine abschließende Stellungnahme liegt mir noch nicht vor, da das Ministerium den Bundesminister der Justiz und die anderen Landesjustizverwaltungen um Stellungnahme zu den aufgeworfenen Grundsatzfragen gebeten hat.

Ein ähnlicher Fall, den mir eine Petentin im Berichtszeitraum unterbreitet hat, verdeutlicht weiter die Dringlichkeit des Schutzes des Persönlichkeitsrechts im gerichtlichen Verfahren: In einer Mietstreitigkeit hatte die Petentin auf Räumung der Wohnung geklagt und sich darauf berufen, im Zeitpunkt des Abschlusses des Mietvertrags nicht geschäftsfähig gewesen zu sein. Auf Anraten ihres Anwalts und mit ihrem Einverständnis wurde ein umfangreiches psychiatrisches Gutachten über ihre Geschäftsfähigkeit zum Zeitpunkt des Vertragsschlusses erstellt, das nach Angaben der Petentin ihre Lebensgeschichte einschließlich ihres Sexuallebens in ihrer Jugend vor 40 Jahren enthielt. Das Gutachten, das entgegen ihrer Erwartung ihre Geschäftsfähigkeit zum Zeitpunkt des Vertragsabschlusses feststellte, wurde vom Gericht dem gegnerischen Anwalt zur Gewährung des rechtlichen Gehörs zugestellt, der es seinem Mandanten zur Verfügung stellte. Seit dieser Zeit wird die Petentin von ihrem damaligen Prozeßgegner, der noch heute ihr Mieter ist, bei jeder Gelegenheit durch hämische Bemerkungen verspottet.

Die Betroffene war weder von ihrem Anwalt noch vom Gericht noch von dem untersuchenden Arzt darauf hingewiesen worden, daß das schriftliche Gutachten zu den Verfahrensunterlagen genommen und ihrem Prozeßgegner zur Kenntnisnahme gelangen würde. Die Betroffene, die durch die Folgen des Gutachtens zutiefst verletzt und gedemütigt ist, hätte sich bei entsprechender Belehrung nicht freiwillig untersuchen lassen.

Auch in diesem Fall bewertet das Gericht den verfassungsrechtlich gebotenen Schutz der Persönlichkeit und der Würde der Betroffenen im Verhältnis zur Gewährung rechtlichen Gehörs für den Prozeßgegner zu gering. Gerade in diesem Fall hätte sich eine Übersendung des Gutachtens an den Prozeßgegner erübrigen können, da die Begutachtung zur Feststellung der Geschäftsfähigkeit der Klägerin geführt hatte und dies im Zivilverfahren für die Betroffene nachteilig war. Nur bei Feststellung der Geschäftsunfähigkeit der Petentin hätte der Prozeßgegner Veranlassung gehabt, sich zu diesem für ihn negativen Umstand zu äußern. Im zugrundeliegenden Fall hätte das Gericht nach Eingang des Gutachtens und angesichts der detaillierten Ausführungen zum Intimleben der Klägerin diese oder ihren Anwalt über das Ergebnis der Begutachtung unterrichten können, so daß diese eine Klagerücknahme hätten erwägen können. Die Zustellung des Gutachtens an den Prozeßgegner und der daraus resultierende Eingriff in das Persönlichkeitsrecht der Klägerin hätte sich dadurch erübrigen können. Schließlich wäre auch hier zu überlegen, ob nicht der Rechtsanwalt des Prozeßgegners als Organ der Rechtspflege es hätte unterlassen müssen, das Gutachten über die Petentin, zumindest in Schriftform, an seinen Mandanten weiterzugeben. Ich habe das Justizministerium gebeten, auch diesen Fall in seine abschließende Stellungnahme zum Problemkreis „rechtliches Gehör und Persönlichkeitsschutz in gerichtlichen Verfahren" einzubeziehen.

6.6.2 Wiedergabe psychiatrischer Gutachten in gerichtlichen Entscheidungen

In einer Eingabe schilderte ein Beklagter eines Privatklageverfahrens, er fühle sich durch die Begründung des die Klage ablehnenden Gerichtsbeschlusses in

seinem Persönlichkeitsrecht beeinträchtigt. Das Gericht hatte die Privatklage zurückgewiesen und dem Privatkläger die Verfahrenskosten auferlegt, da nicht ausgeschlossen werden konnte, daß der beklagte Petent schuldunfähig gewesen war. In der Begründung nahm das Gericht weitgehend Bezug auf das psychiatrische Gutachten über den Petenten, das es dem Beschluß beifügte.

Der Beschluß, der dem Kläger zuzustellen war, enthielt medizinische Einzelheiten über den Gesundheitszustand des Petenten, deren Kenntnis in diesem Umfang für den Kläger aus meiner Sicht nicht erforderlich erscheint. Nach meiner Auffassung hätte es genügt, wenn das Gericht in der Begründung allgemein dargestellt hätte, weshalb es eine Schuldunfähigkeit des Privatbeklagten nicht ausschließen könne. Jedenfalls hätte das Gericht davon absehen sollen, das medizinische Gutachten in Ablichtung beizufügen. Der Schutz des Persönlichkeitsrechts des Betroffenen hätte es erfordert, medizinische Gutachten nur im unerläßlichen Ausmaß zu offenbaren.

Das Staatsministerium der Justiz, das ich auch hierzu um Stellungnahme gebeten habe, verweist darauf, daß die Begründung richterlicher Entscheidungen zum Kernbereich der richterlichen Tätigkeit gehöre. Im Hinblick auf die verfassungsrechtlich gewährleistete Unabhängigkeit der Gerichte könne die getroffene Entscheidung inhaltlich nicht bewertet werden. Dies gelte auch für die Frage, ob in den Gründen die Frage der Schuldfähigkeit anders oder kürzer hätte abgehandelt werden können. Schließlich müsse der Kläger, der mit seiner Klage abgewiesen worden sei, überprüfen können, ob das Gericht zu Recht von einer nicht ausschließbaren Schuldunfähigkeit ausgegangen sei. Würde das Gericht im Interesse des Persönlichkeitsschutzes auf eine eingehende Begründung und Zitierung der gutachtlichen Stellungnahme verzichten, müßte damit gerechnet werden, daß die Partei, die im Verfahren unterlegen sei, sich im Wege der Akteneinsicht die notwendigen Informationen verschaffe.

Auch wenn man davon ausgeht, daß das rechtliche Gehör für den Kläger in diesem Fall die Einsichtnahme in die Prozeßakten und damit in das Gutachten einschließt, ist noch nicht gesagt, daß der Kläger von diesem Recht auch tatsächlich Gebrauch macht und die bloßstellenden Feststellungen des Gutachtens zu seiner Kenntnis gelangen. Das Staatsministerium der Justiz hat die aufgeworfenen Fragen zum Gegenstand einer Richter-Dienstbesprechung gemacht, um auf die zugrundeliegenden Fragen hinzuweisen.

6.7 Datenschutz im Notariat

Nachdem der Bundesgerichtshof in seiner Entscheidung vom 30. Juli 1990 für Nordrhein-Westfalen festgestellt hat, daß das Landesdatenschutzgesetz auch für Notare gilt, habe ich mit dem Staatsministerium der Justiz und der Landesnotarkammer die Konsequenzen dieser Entscheidung für die bayerischen Notare mit folgendem Ergebnis erörtert:

- Das Bayer. Datenschutzgesetz gilt auch für die bayerischen Notare.
- Die bayerischen Notare haben deshalb automatisierte personenbezogene Dateien gem. Art. 7 Abs. 5 BayDSG, § 7 DSRegV zum Datenschutzregister anzumelden. Sie verwenden dabei Formulare, die zwischen dem Bayer. Landesbeauftragten für den Datenschutz und der Landesnotarkammer Bayern abgestimmt sind.
- Zur Wahrnehmung seiner Aufgaben aus dem Datenschutzgesetz steht dem Landesbeauftragten für den Datenschutz im Rahmen der bestehenden datenschutzrechtlichen Bestimmungen ein Zugangs- und Überprüfungsrecht bei den Notariaten zu.

In der Zwischenzeit haben bereits eine Vielzahl von Notaren ihre automatisierten personenbezogenen Dateien bei mir angemeldet. Während somit die Notare ihre Dateien bei meiner Dienststelle anmelden, erkennt die Landesnotarkammer Bayern die Kontrollkompetenz des Landesbeauftragten für den Datenschutz immer noch nicht an. Nach ihrer Auffassung schließe § 18 Bundesnotarordnung — der die Verschwiegenheitspflicht der Notare regelt — eine Offenbarung von individuellen personenbezogenen Angaben und Daten, die bei der Amtstätigkeit des Notars von diesem erhoben und verarbeitet werden, gegenüber dem Landesbeauftragten für den Datenschutz aus. Die Landesnotarkammer Bayern sehe sich außerstande, Befugnisse des Landesbeauftragten für den Datenschutz insoweit anzuerkennen, als sie mit der Kenntnisnahme individueller Angaben über Verhältnisse von Beteiligten an Notargeschäften verbunden seien. Deshalb lege die Landesnotarkammer Bayern größten Wert darauf, daß der Landesbeauftragte eine Datenschutzkontrolle bei Notaren nur im Zusammenwirken mit dem zuständigen Präsidenten des Landgerichts wahrnehmen werde, um die Konfliktlage für den einzelnen Notar lösbar zu gestalten.

Dieser Rechtsauffassung der Landesnotarkammer bin ich in einem Schreiben an das Staatsministerium der Justiz entgegengetreten. Ich habe zwar aus rein praktischen Gründen meine Bereitschaft erklärt, das Ministerium und den Präsidenten des zuständigen Landgerichts von bevorstehenden datenschutzrechtlichen Prüfungen bei Notaren zu unterrichten und diese in Anwesenheit von Vertretern der genannten Stellen durchzuführen, wie dies in ähnlicher Weise auch bei der Kontrolle von Staatsanwaltschaften geschieht. Es wäre aber falsch, darin eine Anerkennung der Einschränkung meiner eigenständigen gesetzlichen Prüfungskompetenz zu sehen. Im Gegensatz zur Landesnotarkammer bin ich der Auffassung, daß die in § 18 Bundesnotarordnung geregelte Verschwiegen-

heitspflicht der Notare einer umfassenden datenschutzrechtlichen Prüfungskompetenz des Landesbeauftragten für den Datenschutz nicht entgegensteht. Diese Pflicht trifft im Grundsatz den gesamten öffentlichen Bereich, ohne daß daraus Einschränkungen der Prüfungskompetenz des Landesbeauftragten für den Datenschutz abgeleitet werden können. Selbst für personenbezogene Daten, die einem besonderen Amtsgeheimnis unterliegen, wie Steuer- und Sozialdaten, ist die Kontrollkompetenz des Landesbeauftragten für den Datenschutz völlig unstrittig. Sogar das Patientengeheimnis kann dem Datenschutzbeauftragten nicht entgegengehalten werden, soweit nicht ein konkreter Widerspruch des Betroffenen vorliegt (§ 24 BDSG). Ebensowenig wie das Steuergeheimnis die Steuerverwaltung, schützt die notarielle Verschwiegenheitspflicht den Notar vor den Kontrollen des Landesbeauftragten für den Datenschutz. Das Staatsministerium der Justiz hat daraufhin gegenüber der Landesnotarkammer geäußert, daß nach seiner Auffassung dem Landesbeauftragten im Rahmen der ihm zugewiesenen Aufgaben ein Zugangs- und Überprüfungsrecht für die Notariate zustehe.

7. Regierungen, Landkreise, Städte und Gemeinden

7.1 Vergabe von Erschließungsbeitragsarbeiten an Privatunternehmen

Durch einen Pressebericht wurde ich darauf aufmerksam, daß eine Gemeinde die Planungs- und Vorbereitungsarbeiten zur Erhebung von Erschließungsbeiträgen sowie deren Berechnung an ein Privatunternehmen vergeben hat. Bei meinen Ermittlungen stellte ich fest, daß dieser Datenverarbeitung im Auftrag ein Vertrag zugrunde lag, durch den die Belange des Datenschutzes völlig unzureichend gewahrt waren. Zwar ist die Vergabe von Aufträgen an Private zur Verarbeitung personenbezogener Daten nicht generell unzulässig. Sollen jedoch sensible Daten wie (z.B. Grundeigentumsverhältnisse) durch Private im Auftrag verarbeitet werden, darf dies nur in unabweisbaren Fällen (z.B. weil die Gemeinde über unzureichende Personalkapazitäten verfügt und keine andere öffentliche Stelle die Auftragsdatenverarbeitung übernehmen kann) und unter strengen Voraussetzungen geschehen. So hat die Gemeinde den Auftragnehmer sorgfältig auszuwählen. Dabei hat sie sich zu vergewissern, daß beim Auftragnehmer ausreichende Datensicherungsmaßnahmen getroffen sind und das Datengeheimnis gewahrt ist. In einer **schriftlichen** Vereinbarung sind die datenschutzrechtlichen Erfordernisse festzulegen. Insbesondere sollten in der Vereinbarung nachstehende Punkte berücksichtigt werden:

- ausreichende Datensicherungsmaßnahmen beim Auftragnehmer (vgl. Art. 15 BayDSG),
- Vertragsstrafen und Bestimmungen über eine fristlose Kündigung bei Verletzungen von Datenschutzvorschriften,
- Datenlöschungsregelung nach Beendigung der übertragenen Arbeiten,
- Zustimmungsvorbehalt für die Gemeinde bei der Einschaltung von Subunternehmen durch den Auftragnehmer,
- Kontrollrecht in datenschutzrechtlicher Hinsicht für die Gemeinde bzw. deren Datenschutzbeauftragten beim Auftragnehmer.

Da die von mir beanstandete Vertragsgestaltung bei der Vergabe von Erschließungsbeitragsarbeiten an Private beileibe kein Einzelfall ist, begrüße ich ausdrücklich das Schreiben des Staatsministeriums des Innern vom 27.04.1989 an die nachgeordneten Behörden, das Hinweise auch zur datenschutzgerechten Vertragsgestaltung in solchen Fällen enthält.

7.2 Prüfung einer Großstadt

Bei einer Großstadt habe ich die Staatsangehörigkeitsstelle, das Gewerbereferat, das Standesamt und die Straßenverkehrsbehörde geprüft. Folgende Mängel waren festzustellen:

- Die Straßenverkehrsbehörde führt eine eigene Urlaubs- und Krankenkartei, in der auch Angaben über **Krankheitsdiagnosen** enthalten waren. Auf einer Karteikarte, die bis in das Jahr 1970 zurückreichte, waren z.B. Diagnosen wie „Brechdurchfall, Erbrechen, Grippe, Erkältung" vermerkt.

  Solche Krankheitsdiagnosen sind für die Personalverwaltung nicht erforderlich. Ich habe die Stadt aufgefordert, die Karteikarten mit den Angaben der Krankheitsdiagnosen zu vernichten und künftig Eintragungen dieser Art zu unterlassen. Die Stadt hat meine Forderungen erfüllt.

- Im Standesamt bin ich auf eine sogenannte „Testamentskartei" gestoßen, aus der entgegen § 324 Abs. 2 Satz 2 der Dienstanweisung für die Standesbeamten aus Personal- und Zeitmangel bisher überholte Karteikarten nicht ausgesondert worden sind. Amtsgerichte und Notare, bei denen ein Testament verwahrt wird, sind verpflichtet, das Standesamt, das die Geburt des Testators beurkundet hat, von der Verwahrung des Testaments zu benachrichtigen. Das Standesamt verwahrt und registriert diese Mitteilungen. Nach dem Tod des Erblassers benachrichtigt das Standesamt den Notar oder das Amtsgericht. Die Karteikarte ist dann noch fünf Jahre (bei Todeserklärung oder gerichtlicher Feststellung der Todeszeit 30 Jahre) aufzubewahren.

Ich habe die Aussonderung und Vernichtung nach Ablauf dieser Fristen gefordert.

- In der Straßenverkehrsbehörde stieß ich auf die Kartei der Fahrlehrer, aus der bisher ebenfalls noch nicht ausgesondert worden ist. Diese Kartei enthielt z.B. auch Fahrlehrer, die längst verstorben oder im Ruhestand waren.

  Ich habe die Bereinigung dieser Kartei gefordert.

- Im übrigen mußte ich auch bei dieser Prüfung wieder feststellen, daß viele sensible Unterlagen ungesichert aufbewahrt waren. Die Stadt hat zwischenzeitlich meine Forderung nach sicherer Aufbewahrung durch Anschaffung geeigneter Stahlschränke erfüllt.

7.3 Prüfung eines Landratsamtes

Bei der Prüfung eines Landratsamtes mußte ich feststellen, daß die Beihilfeverwaltung dem Personalsachgebiet zugeordnet ist.

Zwar ist die für die Beihilfeverwaltung zuständige Mitarbeiterin nicht gleichzeitig mit Personalangelegenheiten befaßt. Dennoch entspricht diese Organisation nicht dem **Gebot der sachlichen und organisatorischen Trennung von Personal- und Beihilfeverwaltung auf Sachgebietsebene**. Die Trennung von Personal- und Beihilfeverwaltung ist deshalb so strikt durchzuführen, weil nur auf diese Weise sichergestellt ist, daß die Beihilfedaten, welche die Bediensteten ausschließlich zum Zwecke der Beihilfegewährung angeben, nur den mit der Beihilfesachbearbeitung befaßten Stellen, insbesondere aber nicht den Personalsachbearbeitern zugänglich sind.

Diese Verstöße überraschen umso mehr, als ich in meinen letzten Tätigkeitsberichten wiederholt auf diese Problematik hingewiesen habe. Ferner hat das Staatsministerium des Innern in seinem 1990 veröffentlichten Mustergeschäftsverteilungsplan die Trennung von Personal- und Beihilfeverwaltung vorgesehen.

Besonders krasse Verstöße gegen die Vorschriften der Datensicherheit traf ich im Sachgebiet „Wohngeld, Unterhaltssicherung" an. In diesem Sachgebiet, das sich mit besonders sensiblen Angelegenheiten zu befassen hat, waren Karteien in **offenen Behältnissen ohne jede Sicherung** untergebracht. Es fehlten an diesen Behältnissen Deckel und Schlösser. Die dazugehörigen Akten befanden sich durchwegs in offenen, nichtabschließbaren Schränken.

Ich habe die Unterbringung der Akten und Karteien beanstandet.

Auch die Unterbringung von Altakten in der Registratur entsprach nicht den Anforderungen der Datensicherheit. In der Registratur befanden sich Akten über abgelehnte Asylbewerber und ausgereiste Ausländer sowie Akten mit Darlehensbescheiden in Bauangelegenheiten. Diese Akten waren in offenen Regalen untergebracht. Die Registratur in diesem Amt befindet sich unmittelbar neben der Kantine und ist keineswegs durchgehend abgeschlossen oder sonst unter Aufsicht. Auch diese Art der Unterbringung habe ich beanstandet.

7.4 Prüfung eines Wasserwirtschaftsamtes

Bei der Kontrolle eines Wasserwirtschaftsamtes waren folgende Mängel festzustellen:

- Die **Arbeitszeiterfassungskarten** der Bediensteten waren nicht vor Unbefugten gesichert. Die Stechkarten, auf denen bereits der volle Name eingetragen war, steckten während und außerhalb der Dienstzeit ungesichert in einem Kartenkasten in unmittelbarer Nähe des Eingangs. Da auf den Zeiterfassungskarten die Uhrzeiten von Dienstbeginn und Dienstende und bereits die Zeitkonten eingetragen waren, konnten die geleisteten Arbeitszeiten, Fehlzeiten, Defizite u.ä. Unbefugten zur Kenntnis gelangen.

  Wenn Zeiterfassungskarten Unbefugten zugänglich sind, dürfen sie an die Bediensteten nicht mit Namen versehen ausgegeben werden. Die Karten dürfen nur mit Nummern oder Buchstabenkombinationen gekennzeichnet den Bediensteten ausgehändigt werden. Es muß die Möglichkeit bestehen, den Namen erst bei der Rückgabe einzutragen.

- Auf dem **Urlaubsverzeichnis** des Amtes waren im Abschnitt „sonstige Fehltage" auch die Krankheitstage vermerkt. Bei einigen Bediensteten waren in der Spalte „Ursache" die Diagnosen (z.B. „Ellenbogenfraktur", „Entfernung Armnagel" u.ä.) angegeben. Da die Angabe der Krankheitsdiagnosen für die Erfüllung der Aufgaben der Personalverwaltung nicht erforderlich ist, habe ich deren Löschung gefordert.

- **Akten** des Wasserwirtschaftsamtes über wasserbauliche Anlagen (Triebwerke, Mühlen u.ä.) waren in den Gängen des Amtes untergebracht, u.a. im Erdgeschoß. Diese Akten befanden sich zwar in verschließbaren Stahlschränken; diese werden aber tatsächlich nicht abgeschlossen, auch nicht nach Dienstschluß. Weil Unbefugte jederzeit Einblick in die Akten nehmen oder sie entwenden konnten, habe ich diese unzureichende Aufbewahrung beanstandet.

  Auf Gängen mit Publikumsverkehr sind Schränke stets **verschlossen** zu halten. Nur befugten Sachbearbeitern darf der Zugriff möglich sein.

- Eine Reihe von Karteien und Ordnern, z.B. ein Verzeichnis der Schwerbehinderten, war in nichtabschließbaren Schränken untergebracht.

7.5 Veröffentlichung eines Untersuchungsberichts

Im 12. Tätigkeitsbericht (Nr. 7.1) habe ich berichtet, daß in einer Stadt ein Untersuchungsbericht, den ein aus Mitgliedern des Stadtrats bestehender Untersuchungsausschuß verfaßt hatte, aus einer nichtöffentlichen Stadtratssitzung an die Öffentlichkeit gelangt ist. Infolge eines Versehens hatte es ferner geheißen, aufgrund der gesamten Umstände sei davon auszugehen, daß ein Mitglied des Untersuchungsausschusses den Bericht der örtlichen Presse zugespielt habe. Eine Überprüfung aufgrund eines Hinweises eines Mitgliedes des Untersuchungsausschusses hat jedoch ergeben, daß neben den Mitgliedern des Untersuchungsausschusses auch die bei der nichtöffentlichen Stadtratssitzung anwesenden Stadtratsmitglieder sowie die mit der Erstellung des Berichts befaßten Bediensteten der Stadtverwaltung als Informanten der Presse in Frage kommen.

7.6 Mieterinformationen in Stadterneuerungsgebieten

Eine kreisfreie Stadt hat bei mir angefragt, ob es zulässig sei, daß das städtische Bauordnungsamt der „Familienhilfe" mitteilt, welche Gebäude von einem Eigentümerwechsel betroffen sind. Die Familienhilfe ist ebenfalls eine städtische Einrichtung und hat nach Angaben der Stadt die Aufgabe, Mietern bei der Vermeidung von nachteiligen Auswirkungen durch städtebauliche Sanierungsmaßnahmen zu helfen.

Das Bauordnungsamt erhält die Mitteilung des bevorstehenden Eigentümerwechsels von den Notaren. Die Notare teilen gem. § 28 Baugesetzbuch der Stadt den Inhalt des Kaufvertrages mit, damit die Stadt prüfen kann, ob sie vom gemeindlichen Vorkaufsrecht Gebrauch macht. Das Bauordnungsamt möchte diese Informationen an die städtische Familienhilfe weiterleiten, die ihrerseits die betroffenen Mieter von dem bevorstehenden Eigentümerwechsel informieren will.

In Übereinstimmung mit dem Staatsministerium des Innern halte ich bereits die Weitergabe der Information vom Bauordnungsamt der Stadt an die Familienhilfe der Stadt für unzulässig.

Wie dargelegt, erhält das Bauordnungsamt der Stadt die Angaben von den Notaren zur Prüfung der Frage, ob die Stadt das gemeindliche Vorkaufsrecht ausüben möchte. **Nur zu diesem Zweck** werden die Daten der Stadt übermittelt. Die Weiterleitung der Daten vom Bauordnungsamt an die Familienhilfe wäre eine zweckwidrige Verwendung, die datenschutzrechtlich nicht zulässig ist. Zu bedenken ist in diesem Zusammenhang auch, daß die Notare verpflichtet sind, die Daten aus den Kaufverträgen an die Gemeinde weiterzugeben. Es handelt sich also nicht um eine freiwillige Datenübermittlung der Notare an die Gemeinden.

Ich habe meine Auffassung der Stadt mitgeteilt.

7.7 Betretungsrecht eines Kontrolleurs der Stadtwerke

Ein Ehepaar hat sich darüber beschwert, daß ein Kontrolleur der Stadtwerke ohne sein Einverständnis die Kellerräume seines Hauses besichtigt habe. Der Kontrolleur sei in das Haus gelangt, weil die Zugehfrau ihm Zutritt verschafft habe.

Meine Ermittlungen haben folgenden Sachverhalt ergeben:

Das Bauordnungsamt der Stadt hatte den Stadtwerken eine Bauveränderungsanzeige für das Anwesen zugeleitet. Aufgrund der baulichen Änderungen mußten die Stadtwerke den Herstellungsbeitrag für das Wasserversorgungsverteilungsnetz, den die Eheleute als Hauseigentümer zu tragen haben, neu berechnen. Der Kontrolleur der Stadtwerke wollte die Umbauten an Ort und Stelle besichtigen.

Die Zuleitung der Bauveränderungsanzeige vom Bauordnungsamt an die Stadtwerke war zulässig, weil die Stadtwerke diese zur Erfüllung ihrer Aufgaben benötigten (Art. 17 BayDSG).

Den Stadtwerken steht auch grundsätzlich ein Zutrittsrecht zu dem Anwesen zu. Dieses Zutrittsrecht ist den §§ 14 und 16 der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser geregelt. Diese Allgemeinen Bedingungen für die Versorgung mit Wasser sind Bestandteil der Vertragsbeziehungen zwischen den Stadtwerken und ihren Kunden. Die Beauftragten der Stadtwerke dürfen die Wohnung der Kunden jedoch nur **mit deren Einverständnis** betreten. Dies folgt aus der grundgesetzlich geschützten Unverletzlichkeit der Wohnung (Art. 13 Grundgesetz).

Das Einverständnis der Eheleute lag in diesem Fall nicht vor.

In der Bereitschaft der Zugehfrau der Eheleute, den Beauftragten der Stadtwerke den Zutritt zu gestatten, kann das Einverständnis nicht gesehen werden. Dazu war die Zugehfrau der Eheleute nicht befugt. Korrekt wäre es gewesen, wenn der Kontrolleur der Stadtwerke nur mit vorheriger Zustimmung der Eheleute das Anwesen betreten hätte. Bei einer rechtzeitigen Terminabsprache wäre dies möglich gewesen. Ich habe meine Auffassung den Stadtwerken mitgeteilt und um künftige Beachtung gebeten.

7.8 Weitergabe von Daten über Einkommensverhältnisse des Mieters an den Vermieter im Zusammenhang mit der Erhebung einer Ausgleichszahlung nach § 7 Wohnungsbindungsgesetz

Das Verfahren zur Erhebung einer Ausgleichszahlung nach § 7 Wohnungsbindungsgesetz, die der **Vermieter** bei Vorliegen der gesetzlichen Voraussetzun-

gen zu zahlen hat, erlaubt dem Vermieter Rückschlüsse auf die Einkünfte seines **Mieters.**

Wohnungen, die dem Wohnungsbindungsgesetz unterliegen, sind öffentlich gefördert und dürfen grundsätzlich nur an solche Personen vermietet werden, die Anspruch auf eine Sozialwohnung haben („Wohnungsberechtigung"). Von dieser Verpflichtung kann sich der Vermieter freistellen lassen. Für diese Freistellung muß der Vermieter unter bestimmten Voraussetzungen eine Ausgleichszahlung leisten. Der Vermieter kann dann vom Mieter neben der Einzelmiete einen entsprechenden Zuschlag verlangen. Die Höhe der Ausgleichszahlung (die vom Wohnungsamt festgelegt wird) bestimmt sich nach der Höhe des Einkommens seines Mieters. Die genaue zahlenmäßige Höhe des Einkommens seines Mieters wird dem Vermieter zwar nicht offenbart. Der Vermieter kann jedoch aus der Höhe der von ihm zu leistenden Ausgleichszahlung Rückschlüsse auf die Höhe des Einkommens seines Mieters ziehen.

Dieses Verfahren halte ich für alles andere als datenschutzfreundlich und habe den Bundesbeauftragten für den Datenschutz gebeten, sich gegenüber dem Bundesminister für Raumordnung, Bauwesen und Städtebau für eine grundlegende Umgestaltung dieser bundesgesetzlichen Regelung einzusetzen.

7.9 Übermittlung der Daten kommunaler Mandatsträger an die Handwerkskammern

Einem Landratsamt kamen Bedenken, ob es der Handwerkskammer (im Benehmen mit einem kommunalen Spitzenverband) zu **statistischen** Zwecken nachstehende Daten kommunaler Mandatsträger mitteilen dürfe: Name, Vornamen, Partei, Beruf, Geburtsjahr, selbständig/unselbständig.

Aus diesen Informationen wollte die Handwerkskammer ersehen, **wie viele Handwerker mit welchem Handwerk und mit welcher Parteizugehörigkeit** in den Gemeinderäten vertreten sind.

Für diesen von der Handwerkskammer verfolgten Zweck, eine Statistik zu erstellen, war jedoch die Mitteilung der Namen und Vornamen der Gemeinderatsmitglieder nicht erforderlich; es genügte die Angabe der **Zahl der Handwerker pro Handwerksart und pro Partei.**

Da die Aktion sämtliche bayerischen Landratsämter und Handwerkskammern betraf, habe ich diese entsprechend unterrichtet und die Handwerkskammern außerdem aufgefordert, die personenbezogenen Mandatsträgerdaten zu löschen.

7.10 Online-Zugriff der Rechnungsprüfungsämter auf Daten der Verwaltung

Eine Stadt fragte mich, unter welchen Voraussetzungen Beamte des Rechnungsprüfungsamtes mittels eines eigenen Terminals auf Dateien der Verwaltung zugreifen dürfen.

In Abstimmung mit dem Staatsministerium des Innern vertrete ich hierzu folgende Auffassung:

Nach Art. 104 Abs. 2 Satz 3 Gemeindeordnung ist das Rechnungsprüfungsamt bei der Wahrnehmung seiner Aufgaben unabhängig und nur dem Gesetz unterworfen. Es bestimmt grundsätzlich Zeitpunkt und Art der Prüfung im Rahmen des Art. 106 Gemeindeordnung selbst, wobei die Befugnisse des ersten Bürgermeisters nach Art. 104 Abs. 2 Satz 4 Gemeindeordnung unberührt bleiben.

Fordert ein Prüfungsbeamter Einsicht in den automatisiert geführten Datenbestand des von ihm zu prüfenden Sachgebiets, so stehen datenschutzrechtliche Bedenken grundsätzlich nicht entgegen. Der Zugang ist jedoch so zu regeln, daß die geprüfte Stelle als speichernde Stelle die datenschutzrechtliche Verantwortung über die gespeicherten Daten nicht verliert. Dabei sind folgende Grundsätze zu beachten:

- Der Online-Zugriff durch den Rechnungsprüfungsbeamten ist — entsprechend seinem Prüfungsauftrag — nur während der Zeit einer Prüfung zulässig. Danach ist die Zugriffsberechtigung zu löschen (Benutzercode, Paßwort). Die Zeitdauer des Zugriffs ist zwischen dem Leiter des zu prüfenden Referats und dem Prüfungsbeamten festzulegen.
- Herr der Daten bleibt das zu prüfende Referat bzw. die zu prüfende Behörde.
- Soweit beim Prüfungsbeamten Bildschirmausdrucke erstellt werden, sind diese — zusammen mit den übrigen Prüfungsunterlagen — datenschutzgerecht aufzubewahren und mittels Reißwolf datenschutzgerecht (DIN 32757) zu vernichten, sobald sie entbehrlich geworden sind.
- **Ändernde** Zugriffe auf den Datenbestand über den Bildschirm des Prüfbeamten sind auszuschließen.
- Über Beginn und Ende sowie über den Benutzer (Prüfungsbeamten) sind für den Zugriffszeitraum Aufzeichnungen zu führen. Insbesondere ist das erteilte Benutzerprofil über die Zugriffsrechte während der Prüfung zu dokumentieren. Fehlerhafte Zugriffsversuche sind aufzuzeichnen.
- Schließlich hat der für das geprüfte Referat zuständige Datenschutzbeauftragte das Verfahren stichprobenweise zu überwachen.

7.11 Auskunft aus der Kaufpreissammlung

Das Staatsministerium des Innern hat mir den Entwurf einer Gutachterausschußverordnung zur Stellungnahme zugeleitet. Die bei den Kreisverwaltungsbehörden bestehenden Gutachterausschüsse haben nach dem Baugesetzbuch u.a. die Aufgabe, sog. „Kaufpreissammlungen" zu führen. Die Kaufpreissammlung unterliegt grundsätzlich der Geheimhal-

tung. Auf Antrag sind aus einer Kaufpreissammlung Auskünfte zu erteilen, soweit ein **berechtigtes Interesse** nachgewiesen wird.

Zu begrüßen ist, daß die Auskünfte aus der Kaufpreissammlung nur bei Vorliegen eines berechtigten Interesses erteilt werden. Dieses Erfordernis macht aber nur Sinn, wenn der auskunftserteilende Bedienstete jeweils prüft, ob ein berechtigtes Interesse vorliegt und die Entscheidung bei einer Kontrolle auch nachvollziehbar ist. Das heißt, das berechtigte Interesse muß sich aus dem Vorgang, insbesondere aus der Begründung des Antrags ergeben. Wird hingegen Auskunft erteilt, ohne daß sich eine Spur von berechtigtem Interesse und die Tatsache der Auskunftserteilung aus dem Akt ergibt, käme dies einer Auskunft an jedermann gleich. Deshalb halte ich es für unumgänglich, daß dieses berechtigte Interesse und die Auskunft auch **dokumentiert** werden. Ich habe deshalb gegenüber dem Staatsministerium des Innern gefordert, in der Gutachterausschußverordnung bzw. in den der Verordnung nachfolgenden Vollzugshinweisen zusätzlich festzuschreiben, daß die Anfragen und das geltend gemachte berechtigte Interesse im Akt festgehalten werden, da ohne dieses Mindestmaß an Dokumentation der ansonsten vorgesehene Geheimhaltungsschutz ins Leere ginge. Wenn dieser Forderung der damit verbundene bürokratische Aufwand entgegengehalten wird, so ist zu bedenken, daß Datenschutz leider nicht umsonst zu haben ist (vgl. auch Nr. 11.2).

7.12 Speicherung von gemeindlichen Sitzungsvorlagen in einem Privat-PC durch ein Mitglied des Gemeinderates

Eine Gemeinde wollte wissen, ob ein ehrenamtliches Gemeinderatsmitglied die gemeindlichen Sitzungvorlagen zu Hause in einen Privat-PC einspeichern dürfe.

Mit dem Staatsministerium des Innern halte ich es weder aus kommunalrechtlichen noch aus datenschutzrechtlichen Gründen für zulässig, daß ein Gemeinderatsmitglied die von der Gemeinde zur Sitzungsvorbereitung übersandten Unterlagen, soweit sie personenbezogene Daten über Dritte enthalten, auf Disketten speichert. Hierdurch erhöht sich die Gefahr, daß die in den Unterlagen enthaltenen vertraulichen Informationen an unbefugte Dritte gelangen. Dies wäre mit der Sorgfalts- und Verschwiegenheitspflicht von Art. 20 Abs. 2 Gemeindeordnung, der die ehrenamtlichen Gemeinderäte unterliegen, nicht vereinbar. Gemäß Art. 20 Abs. 2 Satz 3 Gemeindeordnung sind die Sitzungsunterlagen auf Verlangen des Gemeinderates herauszugeben.

7.13 Umfrage zum Einkaufsverhalten der Bürger

Aus der Zeitung entnahm ich, daß eine Kleinstadt eine Unternehmensberatung mit einer Repräsentativuntersuchung zur wirtschaftlichen Attraktivität der Stadt beauftragt hat. Die Beraterfirma befragte Einzelhändler und Verbraucher über ihr Angebot- und Nachfrageverhalten, z.B. ob und wo noch Lücken im Angebot bestünden. Daneben wurden personenbezogene Daten wie Alter, ausgeübter Beruf, Wohnort und Anzahl der Personen im Haushalt erhoben.

Da bei ähnlichen Umfragen immer wieder einmal Verstöße gegen den Datenschutz festzustellen waren, habe ich mich bei der Stadt wegen Einzelheiten der Befragung erkundigt.

Die mit der Durchführung der Befragung beauftragte Unternehmensberatung hat die Untersuchung wie folgt erläutert:

- Die Umfrage wurde anhand von Fragebögen durchgeführt.
- Auf die Freiwilligkeit der Angaben wurden die einzelnen Personen bzw. Betriebsinhaber hingewiesen.
- Bei der **Konsumentenbefragung** wurde von Anfang an auf eine Namensnennung verzichtet.
- Dagegen erfolgte die **Unternehmerbefragung** zunächst betriebsbezogen. In einem persönlichen Gespräch sowie per beigelegtem Anschreiben wurden die Unternehmen über Sinn und Zweck der Untersuchung informiert.
- Die an die Unternehmensberatung zurückgesendeten Fragebögen wurden mit den Adressen der Personen verglichen, die Fragebögen erhalten hatten (sog. Rücklaufkontrolle).
- Unternehmer, die nicht geantwortet hatten, wurden ein zweites Mal angeschrieben.
- Die Rückgabe der Fragebögen erfolgte mittels Freikuvert auf dem Postweg.
- Die zurückgesendeten Fragebögen wurden bei der Eingabe in das Auswertungsprogramm anonymisiert.
- Bei der Auswertung der Ergebnisse will die Unternehmensberatung auf die Veröffentlichung der Leistungskennzahlen von Branchen verzichten, in denen weniger als drei Unternehmen vertreten sind oder ein Marktführer dominiert. Damit soll vermieden werden, daß ortsbekannte Betriebe auch ohne Namensnennung erkannt werden und damit ihre Wirtschaftskraft aus den Zahlen ersichtlich ist.

Soweit die obigen Vorgaben eingehalten werden, bestehen gegen die Durchführung der Marktuntersuchung keine Bedenken.

7.14 Betriebsbefragung in der Landwirtschaft und im Gartenbau

Eine Stadt bat mich um datenschutzrechtliche Bewertung einer beabsichtigten Betriebsbefragung zur Situation der Landwirtschaft in einem ihrer Ortsteile. Die Befragung sollte im Auftrag der Stadt von einer Privatfirma durchgeführt werden. Der hierfür entwikkelte Fragebogen sah u.a. Fragen zur Betriebsnachfolge, zu den Eigentumsverhältnissen sowie zu den künftigen Planungen vor, ferner personenbezogene Angaben wie Name, Altersgruppe, Anschrift und Flurnummer sowie Namen, Geburtsjahr, Tätigkeit und Staatsangehörigkeit der Haushaltsmitglieder. Im „Fragebogen für Gewerbebetriebe" war außerdem nach dem Namen des Betriebes und des Betriebsinhabers, den Eigentumsverhältnissen, der Zahl der Beschäftigten, dem Zustand sowie der künftigen Entwicklung des Betriebes gefragt.

Wegen der zum Teil sehr sensiblen Fragen habe ich gefordert, neben dem bereits vorhandenen Hinweis auf die Freiwilligkeit der Befragung zumindest auf die Namens- bzw. Betriebsangaben zu verzichten. Auch hat die Stadt als auftraggebende Stelle die zweckgebundene Nutzung der personenbezogenen Daten durch die von ihr beauftragte Firma sicherzustellen, beispielsweise durch Androhung einer Vertragsstrafe oder durch entsprechende Kontrollen.

Inzwischen hat die Stadt von der Befragung aus finanziellen Gründen abgesehen.

8. Einwohnermeldewesen

8.1 Rechtliche Entwicklung

Ein neuer Entwurf der Bundesregierung zur Änderung des **Melderechtsrahmengesetzes** (Stand 30.07.1991) zielt u.a. darauf ab, dem Recht des Bürgers auf informationelle Selbstbestimmung im Meldewesen noch stärker Geltung zu verschaffen und die Datenerhebung und -verarbeitung durch Melde- und Sicherheitsbehörden weiter einzuschränken:

- Das Einsichtsrecht der Sicherheitsbehörden in **Patientenverzeichnisse** der Krankenhäuser wird auf Einzelfälle begrenzt.
- Bundesweit soll ein **Widerspruchsrecht** für die Betroffenen gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeführt werden, wie es im Bayer. Meldegesetz bereits seit 01.04.1983 besteht.

Diese Entwicklung begrüße ich.

Derzeit haben die beherbergten Personen, die nicht bei der Meldebehörde anzumelden sind, Meldevordrucke handschriftlich auszufüllen und zu unterschreiben. Beherbergte **Ausländer** müssen sich künftig gegenüber dem Leiter der Beherbergungsstätte oder seinem Beauftragten durch die Vorlage eines gültigen Identitätsdokuments ausweisen.

Die beabsichtigte Regelung entspricht Art. 45 Abs. 1 a des Schengener Zusatzabkommens, wonach eine Identitätsprüfungspflicht der Leiter von Beherbergungsstätten für Ausländer vorgesehen ist. Der Bundesinnenminister führt zur Begründung dieser Identitätsprüfungspflicht u.a. folgendes aus:

„Die beabsichtigte Identitätsprüfungspflicht bei Ausländern erweitert somit u.a. den Pflichtenkreis der Leiter von Beherbergungsstätten. Sie haben nach dem Wortlaut der in Aussicht genommenen Vorschrift künftig darauf „hinzuwirken", daß sich beherbergte Ausländer ihnen gegenüber durch Vorlage eines gültigen „Identitätsdokuments" ausweisen müssen. Unter „Hinwirken" ist dabei die Aufforderung zur Vorlage eines Identitätspapiers zu verstehen.

... Die Leiter von Beherbergungsstätten oder ihre Beauftragten sind gehalten, die im Meldevordruck angegebenen Daten mit denen des Identitätspapiers zu vergleichen. Es ist nicht daran gedacht, im Rahmen der Identitätsprüfungspflicht dem Hotelier umfassende Kontrollfunktionen zu übertragen."

Mit dieser Regelung soll neben anderen Maßnahmen das Sicherheitsdefizit ausgeglichen werden, das durch den Wegfall der EG-Binnengrenzen und der damit verbundenen Grenzkontrollen entstehen wird.

8.2 Prüfungen

Wie in den vergangenen Jahren habe ich die Überprüfung von Einwohnermeldeämtern samt den dort eingesetzten automatisierten Verfahren fortgesetzt. Schwerpunktmäßig umfaßte die Überprüfung die Rechtmäßigkeit und Erforderlichkeit der bei den größeren Städten **selbst** entwickelten Einwohnerverfahren. Mittlerweile habe ich 17 unterschiedliche Verfahren (9 private Softwarehersteller, 8 kommunale Eigenentwicklungen) überprüft und kann feststellen, daß — von Ausnahmen abgesehen — insbesondere die von öffentlichen Stellen entwickelten Programme zwar nicht gänzlich mängelfrei, jedoch im Hinblick auf Rechtmäßigkeit und Erforderlichkeit den Verfahren privater Anbieter vorzuziehen sind. Dies liegt wohl darin begründet, daß die kommunalen Eigenentwicklungen bereits in der Organisationsphase von den Erfahrungen des fachlich kompetenten (Meldeamts-)Personals profitieren. Für ein automatisiertes Einwohnerwesen ist entscheidend, daß nicht nur der Datensatz den gesetzlichen Vorgaben entspricht, sondern daß Inhalt und Bedeutung des **gesamten** Melderechts erkannt und unter Beachtung der rechtlichen Auswirkungen in die Programme eingebettet werden.

Nicht von ungefähr habe ich deshalb in meinen letzten drei Tätigkeitsberichten über die immer wieder festgestellten, typischen Verfahrensmängel berichtet

und erwartet, daß die Softwarehersteller für die von mir noch nicht geprüften Programme die notwendigen Konsequenzen ziehen. Leider hat sich diese Hoffnung nicht in allen Fällen erfüllt.

Erfreulich ist jedoch, daß die früher geprüften und beanstandeten Verfahren von den Softwareherstellern weitgehend bereinigt wurden, so daß deren Kunden von den Verbesserungen profitieren.

8.3 Datenschutz-Verstöße und Probleme des Melderechts — Einzelfälle

Neben der globalen Überprüfung der unterschiedlichen automatisierten Einwohnermeldeverfahren hatte ich mich auch mit zahlreichen Einzelproblemen auseinanderzusetzen.

8.3.1 Gesetzlicher Vertreter im Datensatz eines polizeilich Gesuchten

Ein Bürger wandte sich an mich mit folgendem Anliegen:

Die Polizei habe bei ihren Ermittlungen gegen einen mutmaßlichen Straftäter, dessen Aufenthalt unbekannt sei, unter Berufung auf eine Melderegisterauskunft Hinweise erhalten, die ihn als „Vater" des Gesuchten auswiesen. Er möge sich zum derzeitigen Aufenthalt seines „Sohnes" äußern. Der Petent bat mich festzustellen, ob seine Daten zu Unrecht im Zusammenhang mit dem Straftäter in den Polizeiunterlagen enthalten seien.

Tatsächlich war im Meldedatensatz des mutmaßlichen Straftäters ein Hinweis (Ordnungsmerkmal) enthalten, der den Petenten fälschlicherweise als „Vater" (gesetzlicher Vertreter) des Gesuchten identifizierte. Aufgrund der Melderegisterauskunft versuchte die Polizei vom Petenten den Aufenthalt seines „Sohnes" zu erfahren.

Was war geschehen?

Die für den betreffenden Regierungsbezirk zuständige Datenzentrale der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) hatte das Ordnungsmerkmal des inzwischen verstorbenen echten Vaters des mutmaßlichen Straftäters an den Petenten, der zufällig das gleiche Geburtsdatum wie der Verstorbene hat, wieder vergeben, aber im Datensatz des Gesuchten nicht gelöscht. Dadurch entstand ein Querverweis zwischen dem Datensatz des Gesuchten und dem des Petenten.

Die beteiligten Meldebehörden und die Polizei wurden von mir aufgefordert, ihre Dateien und Unterlagen so zu bereinigen, daß zwischen dem mutmaßlichen Straftäter und dem Petenten keine Verbindung mehr hergestellt werden kann. Die AKDB hat mir hierzu versichert, daß Ordnungsmerkmale des Einwohnermeldewesens seit geraumer Zeit — z.B. nach Freiwerden durch Tod — kein zweites Mal vergeben werden. Darüber hinaus wurde durch programmtechnische Maßnahmen gewährleistet, daß auch bei noch weiter zurückliegenden Fällen keine falschen Querverweise mehr auftreten können. Verwechslungen der bezeichneten Art dürften dadurch künftig ausgeschlossen sein.

8.3.2 Meldedatenübermittlung an das Jugendamt zur Vaterschaftsfeststellung

Eine Meldebehörde fragte, ob es zulässig sei, einem Amtspfleger bei einem Kreisjugendamt in einer Vaterschaftssache die Namen und Anschriften aller männlichen Personen mit Vornamen „M.", die zwischen 1958 und 1963 geboren sind, aus dem Melderegister zu übermitteln.

Nach Auskunft des Amtspflegers sollten die so ermittelten Personen auf freiwilliger Basis zu einer Gegenüberstellung mit der Kindsmutter vorgeladen werden. Meine Frage, ob sich diejenigen, die der Vorladung nicht „freiwillig" Folge leisten, besonders verdächtig machen, konnte mir nicht beantwortet werden.

Die von der Meldebehörde vorgetragenen Bedenken, daß nämlich schutzwürdige Belange der Betroffenen beeinträchtigt werden könnten, teile ich. Es wäre zu befürchten, daß alle „M." der bewußten Jahrgänge bis zur Feststellung des Vaters als potentielle Kindsväter beim Jugendamt gespeichert würden. Außerdem dürfte ein nicht unbeträchtlicher Teil der Betroffenen bereits verheiratet sein, so daß eine Vorladung des Jugendamtes zur Vaterschaftsfeststellung geeignet ist, den häuslichen Frieden zu stören.

Den Sachverhalt einschließlich meiner Bedenken habe ich den Staatsministerien des Innern und für Arbeit, Familie und Sozialordnung geschildert und bin unter Einbeziehung von deren Stellungnahmen zu folgendem Ergebnis gelangt:

Ein nach § 55 Kinder- und Jugendhilfegesetz bestellter Amtspfleger wird stets **im Namen** des unehelichen Kindes tätig und ist melderechtlich als Privatperson (also nicht als Behörde) anzusehen. Die beantragte Gruppenauskunft ist deshalb an Art. 34 Abs. 3 Meldegesetz und nicht an Art. 31 Meldegesetz zu messen. Die dort aufgeführten Kriterien für Gruppenauskünfte sehen eine Auswahl nach „Vornamen" nicht vor, so daß die Auskunft über die in Frage kommenden „M." nicht erteilt werden darf. Dies habe ich der Meldebehörde und dem Amtspfleger mitgeteilt.

8.3.3 Wähleradressen an politische Parteien und Wählergruppen

Mit der Überlassung von Wähleradreßdaten an politische Parteien und Wählergruppen habe ich mich im 12. Tätigkeitsbericht eingehend auseinandergesetzt. Trotzdem sind im Berichtszeitraum wieder einige Verstöße gegen Art. 35 Abs. 1 Meldegesetz bekanntgeworden.

- Das Meldeamt einer Gemeinde hat einem Gemeinderatsmitglied, das für den **Seniorenbeirat** kandidierte, die Anschriften aller Senioren mitgeteilt. Diese Datenweitergabe war unzulässig, weil Art. 35 Abs. 1 MeldeG nur die Wählerauskunft im Zusammenhang mit **allgemeinen** Wahlen und Abstimmungen erlaubt. Hierzu gehören Europa-, Bundestags-, Landtags- und Kommunalwahlen sowie eine Volksabstimmung, nicht hingegen Wahlen von kommunalen Beiräten, wie Ausländerbeiräte und Seniorenbeiräte. Hierauf habe ich die Gemeinde hingewiesen.

- Der Presse war zu entnehmen, daß die Meldebehörde einer Stadt einer politischen Partei auch die Daten Minderjähriger (also noch nicht Wahlberechtigter) zur Verfügung gestellt habe. Meine Nachforschungen bei der Stadt brachten allerdings noch mehr Fehler bei der Datenweitergabe an die politische Partei ans Tageslicht. Außer den Adressen Minderjähriger wurden auch die Daten von nicht wahlberechtigten erwachsenen Personen, aber auch von Personen, die der Weitergabe ihrer Daten widersprochen hatten, übermittelt.

  Diese fehlerhafte Datenweitergabe war auf unsachgemäße Eintragungen in einem Eingabebeleg für die EDV zurückzuführen. Ich habe die Stadt beanstandet und aufgefordert, das für das Einwohnermeldewesen verantwortliche Personal nachdrücklich zur Beachtung der Vorschriften des Melderechts einschließlich des angewandten EDV-Verfahrens anzuhalten, um künftige Fehleingaben der bezeichneten Art möglichst zu vermeiden.

8.3.4 Datenübermittlung an Adreßbuchverlage

Nach Art. 35 Abs. 3 MeldeG darf die Meldebehörde Adreßbuchverlagen Auskunft erteilen über Namen, Vornamen und akademische Grade sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben. Die Betroffenen haben ein Recht, der Weitergabe ihrer Daten zu widersprechen.

Obwohl ein Petent nachweislich wiederholt der Weitergabe seiner Daten an Adreßbuchverlage **widersprochen** hatte, erschienen seine Daten gleichwohl im Adreßbuch.

Meine Ermittlungen bei der Meldebehörde ergaben, daß dort außergewöhnlich geschlampt worden war. Weder war der Widerspruch im Melderegister gespeichert, noch war der Schriftwechsel zwischen dem Petenten und der Meldebehörde auffindbar. Der zwischenzeitlich abgelöste verantwortliche Bedienstete konnte sich an nichts erinnern. Ich habe die Meldebehörde beanstandet und veranlaßt, daß die Auskunftssperre im Datensatz des Petenten gespeichert wurde.

Bei meiner Kontrolle dieser Meldebehörde stellte ich ferner fest, daß auch die Bestimmungen zu „Melderegisterauskünften über **JVA-Insassen** und über **Behinderte** in Behindertenheimen" nicht beachtet wurden. So fand ich bei meiner Prüfung unter den — zumindest regional allgemein bekannten — Anschriften entsprechender Einrichtungen im Adreßbuch die Namen von JVA-Insassen und Behinderten. In einem anderen Fall fand ich die Daten von Patienten eines Bezirkskrankenhauses im Adreßbuch veröffentlicht. Beide Behörden wurden beanstandet.

Deshalb weise ich nochmals darauf hin, daß das Meldegesetz in diesen Fällen Auskünfte (hier an den Adreßbuchverlag) nur dann erlaubt, wenn die Meldebehörde durch **Prüfung im Einzelfall** festgestellt hat, daß schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Vor Melderegisterauskünften ist der Betroffene (JVA-Insasse oder Patient des Bezirkskrankenhauses oder ähnlicher Einrichtungen) zu hören (Art. 25 Abs. 4, Art. 28 Abs. 1 Satz 5 MeldeG).

Allen Meldebehörden ist deshalb zu empfehlen, bei dem betroffenen Personenkreis von Amts wegen eine **Auskunftssperre** nach Art. 35 Abs. 3 MeldeG (keine Melderegisterauskunft an Adreßbuchverlage) zu speichern.

8.3.5 Gruppenauskünfte

Nach Art. 34 Abs. 3 MeldeG darf die Meldebehörde Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner, die einer bestimmten Gruppe angehören (z.B. Gruppenauskunft über alle über 60jährigen) nur erteilen, soweit die Auskunft im öffentlichen Interesse (d.h. im überwiegenden Allgemeininteresse) liegt. Zusätzlich bedarf eine solche Gruppenauskunft gemäß Nr. 34.6 VollzBekMeldeG der Zustimmung der Regierung.

Dagegen haben Gemeinden auch im Berichtszeitraum wiederholt verstoßen.

Beispielsweise hat eine Meldebehörde dem Seniorenclub und der Landjugend die Adressen aller über 60jährigen mitgeteilt, damit man sie zur Adventsfeier oder zu einem Altennachmittag einladen könne.

Nun ist es sicher zu begrüßen, wenn sich in einer Gemeinde Vereine, Gruppen und Initiativen um die älteren Menschen kümmern, damit sie nicht vereinsamen. Durch persönliche, schriftliche Einladungen wird mehr Bereitschaft und Interesse an angebotenen Veranstaltungen geweckt als durch Zeitungsinserate, Informationstafeln, Hinweise im Gemeindeblatt u.ä. Im öffentlichen Interesse liegt die Herausgabe der Adreßdaten an Dritte dennoch nicht. Denn zum einen können Einladungen zu diesen Veranstaltungen auch so organisiert werden, daß die Adressen nicht in die Hände der Veranstalter gelangen. Zum anderen haben die Betroffenen auch ein Recht darauf, daß ihre Zugehörigkeit zur Gruppe der über 60jährigen Dritten nur bei überwiegendem Allgemeininteresse bekannt wird. Dazu gehört die Einladung zu einer Adventsfeier, zu einem Altennachmittag oder zu ei-

ner sonstigen Veranstaltung, wenn sie von privaten Dritten organisiert wird, meiner Auffassung nach nicht. Jeder hat auch das Recht, von solchen persönlichen Einladungen durch Dritte unbehelligt zu bleiben. Im übrigen erfolgte die Adressenweitergabe auch **ohne Zustimmung der Regierung**. Die Weitergabe der Daten entgegen Art. 34 Abs. 3 MeldeG und auch ohne Zustimmung der zuständigen Regierung habe ich beanstandet.

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

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

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

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

8.3.7 Adressenübermittlung an die Polizei zur Nachwuchswerbung für den Polizeivollzugsdienst

Nach Art. 31 Abs. 1 MeldeG darf die Meldebehörde einer anderen Behörde Meldedaten übermitteln, wenn dies zur rechtmäßigen Aufgabenerfüllung des Datenempfängers erforderlich ist.

Ein Polizeipräsidium, das unter akutem Nachwuchsmangel leidet, erhält vom Meldeamt unter Berufung auf diese Bestimmung jährlich die Daten der jungen Männer, die zur Wehrerfassung heranstehen. Seit der Öffnung des Polizeivollzugsdienstes auch für Frauen fordert das Polizeipräsidium auch die Daten der gleichaltrigen jungen Frauen an.

Die vom Staatsministerium des Innern für zulässig gehaltene Adreßübermittlungen habe ich wie folgt bewertet: Im Hinblick auf die besonders prekäre Situation des betreffenden Polizeipräsidiums halte ich die Übermittlung der Daten der zur Wehrerfassung heranstehenden jüngeren Männer sowie der gleichaltrigen Frauen für vertretbar, zumal es zur rechtmäßigen Aufgabenerfüllung der Polizei (hier Aufrechterhaltung der öffentlichen Sicherheit und Ordnung) erforderlich ist, ausreichenden Nachwuchs zu gewinnen.

Allerdings darf die Übermittlung der Adreßdaten nur als letztes Mittel und erst nach Ausschöpfung aller anderen Werbemaßnahmen in Frage kommen. Das gilt insbesondere für die Übermittlung der Adressen der jungen Frauen. Unter der Voraussetzung, daß die Daten der jungen Leute nach Abschluß der Werbeaktion zuverlässig gelöscht werden, werde ich mich bis auf weiteres nicht gegen die Datenübermittlung wenden.

9. Ausländerwesen

9.1 Neues Ausländergesetz

Das neue Ausländergesetz ist am 01.01.1991 in Kraft getreten. Es enthält u.a. Vorschriften über Datenübermittlungen an Ausländerbehörden (§§ 76, 77 Ausländergesetz). Z.B. haben danach öffentliche Stellen die zuständige Ausländerbehörde zu unterrichten, wenn sie Kenntnis erlangen

- vom Aufenthalt eines Ausländers, der weder eine erforderliche Aufenthaltsgenehmigung noch eine Duldung besitzt,
- vom Verstoß gegen eine räumliche Aufenthaltsbeschränkung
  oder
- von einem sonstigen Ausweisungsgrund.

Die für die Einleitung und Durchführung eines Straf- und Bußgeldverfahrens zuständigen Stellen haben die zuständige Ausländerbehörde über die Einleitung des Verfahrens sowie die Verfahrenserledigungen (Verurteilungen, Freisprüche, Einstellungen) bei der Staatsanwaltschaft, bei Gericht oder bei der für die Verfolgung und Ahndung der Ordnungswidrigkeit zuständigen Verwaltungsbehörde zu unterrichten. Meldebehörden, Staatsangehörigkeitsbehörden, Paß- und Personalausweisbehörden, Sozial- und Jugendämter, Arbeitsämter, Finanzämter und Gewerbebehörden haben den Ausländerbehörden personenbezogene Daten von Ausländern, Amtshandlungen und sonstige Erkenntnisse über Ausländer mitzuteilen, soweit diese Angaben zur Erfüllung der Aufgaben der Ausländerbehörden erforderlich sind.

Die Ausländerbehörden benötigen solche Angaben beispielsweise zur Beurteilung der Frage, ob eine Aufenthaltsgenehmigung zu verlängern, eine Aufenthaltserlaubnis zu versagen, oder ein Ausländer wegen Beeinträchtigung der öffentlichen Sicherheit und Ordnung auszuweisen ist.

Ich habe zu diesen Vorschriften im Bayerischen Landtag und bei den Beratungen der Allgemeinen Verwaltungsvorschriften zum Ausländergesetz gegenüber dem Innenministerium folgende Auffassung vertreten:

Wenn sich der Bundesgesetzgeber für einen effektiven Vollzug des Ausländergesetzes entschieden hat, dann ist diese demokratische Entscheidung zu respektieren. Für einen effektiven Vollzug sind Mitteilungspflichten öffentlicher Stellen unabdingbar, damit die zur Entscheidung zuständigen Ausländerbehörden von ausländerrechtlich relevanten Sachverhalten erfahren, die anderen öffentlichen Stellen in Erfüllung ihrer Aufgaben zur Kenntnis gelangt sind. Diese Mitteilungspflichten gelten jedoch nicht schrankenlos. Vielmehr ist auch hier der **Grundsatz der Verhältnismäßigkeit** zu beachten. Unter diesem Gesichtspunkt habe ich folgende einschränkende Interpretation der neuen Vorschriften gefordert, die in Verwaltungsvorschriften niedergelegt werden muß:

- Datenübermittlungen an die Ausländerbehörde müssen im Hinblick auf die möglichen Ausweisungsgründe auf das notwendige Maß beschränkt bleiben. Umstände, die erfahrungsgemäß zu keinem Ausweisungsverfahren führen, dürfen erst gar nicht an die Ausländerbehörden mitgeteilt werden.
- Die Pflicht zur Mitteilung über den Bezug von Sozialhilfe und Jugendhilfeleistungen hängt von Art und Höhe der Leistungen sowie vom Aufenthaltsstatus ab.
- Der Begriff der öffentlichen Stelle, die einen ausweisungsrelevanten Sachverhalt an das Ausländeramt zu übermitteln hat, ist restriktiv auszulegen.
- Der Umfang der innerbehördlichen Schweigepflichten insbesondere der Ärzte und Sozialarbeiter muß klar und eindeutig gegenüber ihrer amtlichen Tätigkeit abgegrenzt werden.

Während des Berichtszeitraumes wurden für Einzelbereiche des Ausländergesetzes vorläufige Vollzugsvorschriften erlassen. Die allgemeinen Verwaltungsvorschriften stehen noch aus.

9.2 Entwurf eines Ausländerzentralregistergesetzes

Im Berichtszeitraum hat der Bundesminister des Innern den Entwurf eines Ausländerzentralregistergesetzes vorgelegt. Mit dem Gesetz soll das seit 1967 in einem automatisierten Verfahren beim Bundesverwaltungsamt geführte Ausländerzentralregister auf eine gesetzliche Grundlage gestellt werden. Im Ausländerzentralregister sind im wesentlichen alle in der Bundesrepublik Deutschland lebenden Ausländer sowie die Ausländer gespeichert, die einen Asylantrag gestellt haben.

Der nunmehr vorgelegte Gesetzentwurf enthält eine Reihe von Verbesserungen gegenüber einem Entwurf aus dem Jahr 1988. Er enthält **Protokollierungsvorschriften** hinsichtlich Datenübermittlungen von Ausländerbehörden, wie ich sie in der Stellungnahme zum früheren Entwurf nachdrücklich verlangt hatte. Zum jetzigen Gesetzentwurf habe ich gefordert, daß die Pflicht zur Löschung von Daten, die für die Aufgabenerfüllung nicht mehr erforderlich sind oder deren Speicherung unzulässig war, klar festgelegt wird.

In der Anhörung ist die Einrichtung eines Ausländerzentralregisters von einigen Landesbeauftragten als Diskriminierung der ausländischen Mitbürger in Frage gestellt worden. An der Erforderlichkeit eines solchen Registers für die Arbeit der Ausländerbehörden und der anderen, mit Ausländern befaßten Dienststellen kann es jedoch keinen Zweifel geben. Manche grundsätzlichen Bedenken anderer Datenschutzbeauftragten gegen das Ausländerzentralregister kann ich nicht teilen:

- § 3 Abs. 2 Nr. 5 sieht vor, daß im Register Daten von Ausländern gespeichert werden, die zur Festnahme oder Aufenthaltsermittlung ausgeschrieben sind. Dagegen wird vorgebracht, mit der Speicherung solcher Daten würden die Ausländerbehörden über ihre eigentlichen Aufgaben hinaus dazu aufgerufen, polizeiliche Aufgaben wahrzunehmen.

  Dem ist nicht so. Die Übermittlung und Speicherung des Bestehens einer Ausschreibung zur Festnahme oder einer Aufenthaltsermittlung dient dem Vollzug des Ausländerrechts. Die Kenntnis solcher Umstände ist zur Aufgabenerfüllung der mit Ausländerrecht befaßten Stellen notwendig.

- Nach § 3 Abs. 2 Nr. 6 sind im Register Daten von Ausländern zu speichern, deren Erfassung erforderlich ist, weil tatsächliche Anhaltspunkte für den Verdacht bestehen, daß sie bestimmte Straftaten planen, begehen oder begangen haben.

  Dagegen wird vorgebracht, dies sei eine Sonderregelung zu Lasten von Ausländern (weil eine solche Regelung für deutsche Staatsangehörige nicht existiert), die dem Legalitätsprinzip und dem Gleichheitsgrundsatz widerspräche.

  Die Speicherung von kriminellen Ausländern im Ausländerzentralregister ist jedoch erforderlich, damit bei Ein- oder Ausreise des Ausländers und bei Anfragen von Ausländerbehörden das Vorliegen besonderer Gefährdungstatbestände sofort erkannt werden kann. Eine Speicherung von Deutschen im Ausländerzentralregister kommt naturgemäß nicht in Betracht. Weshalb hierin eine Diskriminierung von Ausländern liegen soll, ist unerfindlich.

- § 7 Abs. 5 sieht die Zulässigkeit von Gruppenauskünften über Ausländer vor. Gruppenauskünfte sind Auskünfte über eine Mehrzahl von Personen, die nicht namentlich bezeichnet sind und die aufgrund von gemeinsamen Merkmalen zu einer Gruppe gehören.

  Hiergegen wird eingewendet, bei diesen Gruppenauskünften handle es sich um „Rasterfahndungen". Abgesehen davon, daß der Begriff „Rasterfahndung" bereits für völlig anders geartete Maßnahmen der Polizei besetzt ist, sind Bedenken gegen Gruppenauskünfte sachlich unbegründet: Mit Hilfe der Gruppenauskünfte sollen beispielsweise

die Ausländer erfaßt werden, die demnächst wegen Erreichens des 16. Lebensjahres eine Aufenthaltsgenehmigung brauchen. Dieser Personenkreis kann dann darauf hingewiesen werden, daß er für einen weiteren Aufenthalt eine Aufenthaltsgenehmigung zu beantragen habe.

9.3 ED-Behandlung von Asylbewerbern

Die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) hat am 3. Mai 1991 beschlossen, „das erkennungsdienstliche Material **aller** Asylantragsteller zu erfassen". Hintergrund des IMK-Beschlusses waren Feststellungen in mehreren Bundesländern, daß zahlreiche Asylbewerber gleich bei mehreren Sozialhilfebehörden unter verschiedenen Namen Sozialhilfe beantragt und erhalten oder auch gleichzeitig mehrere Asylanträge gestellt haben.

Bei der erkennungsdienstlichen Behandlung (ED-Behandlung) von Asylbewerbern werden sowohl Bundes- wie Landesbehörden tätig. Ihre Rechtsgrundlage hat die ED-Behandlung nicht im Polizeiaufgabengesetz oder in der Strafprozeßordnung, sondern in § 13 Asylverfahrensgesetz. Danach ist die Identität des Asylbewerbers durch erkennungsdienstliche Maßnahmen zu sichern, wenn sie nicht eindeutig bekannt ist. Damit soll sichergestellt werden, daß Asylbewerber nicht unter einer anderen Identität weitere Asylanträge stellen oder Sozialhilfeleistungen mehrmals erhalten.

Entsprechend diesem Regelungszweck ist § 13 AsylVfG weiter gefaßt als § 41 Ausländergesetz, der eine ED-Behandlung davon abhängig macht, daß Zweifel über die Person oder Staatsangehörigkeit eines Ausländers bestehen. Im Gegensatz zu § 41 Ausländergesetz setzt also eine ED-Behandlung von Asylbewerbern keine auf tatsächlichen Anhaltspunkten beruhenden Zweifel an der Identität des Asylbewerbers voraus. Es genügt vielmehr, daß die Behörde sich keine positive Gewißheit von der Identität des Asylbewerbers verschaffen kann. Diese Voraussetzung ist bei Asylbewerbern in aller Regel gegeben. Angesichts der tatsächlichen und rechtlichen Verhältnisse in den Ländern, aus denen die Asylbewerber überwiegend stammen, sowie angesichts der zahlreichen Vorteile, die für einen Asylbewerber mit einem Aufenthalt in Deutschland verbunden sind, kann die Ausländerbehörde nur in Ausnahmefällen davon ausgehen, daß die vorgelegten Ausweispapiere die Identität des Asylbewerbers auch eindeutig bescheinigen. Hinzu kommt, daß es in manchen Staaten, z.B. in der Türkei und in Ghana, nach deren Rechtsordnung ohne besondere Formalitäten oder Schwierigkeiten möglich ist, sich Ausweispapiere unter verschiedenen Namen zu beschaffen. Die Rechtsordnungen dieser Länder ermöglichen somit den legalen Besitz von mehreren Pässen mit verschiedenen Personalien.

Aus diesen Gründen hat das Innenministerium in einer bis 1. Juli 1993 verlängerten Anweisung verfügt, daß die bayerischen Ausländerbehörden grundsätzlich eine ED-Behandlung von Asylbewerbern vorsehen, jedoch bei nachfolgenden Gruppen davon absehen können, sofern im Einzelfall aufgrund der vorgelegten Ausweispapiere keine Zweifel über die Person oder die Staatsangehörigkeit bestehen:

- Staatsangehörige der Mitgliedstaaten der EG
- Ehegatten von Deutschen
- Kinder unter 16 Jahren
- Inhaber einer gültigen Aufenthaltsberechtigung
- Inhaber einer gültigen unbefristeten Aufenthaltserlaubnis
- Personen, die sich unmittelbar vor der Antragstellung ununterbrochen mindestens 1 Jahr erlaubt im Bundesgebiet aufgehalten haben
- Ehegatten von Asylberechtigten
- Personen, die von der Bundesrepublik Deutschland aus humanitären Gründen im Rahmen besonderer Aufnahmeaktionen aufgenommen wurden.

Diese Verfahrensweise steht nach meiner Auffassung mit der gesetzlichen Regelung **in Einklang**.

Die ED-Behandlung besteht darin, daß die Asylbewerber zur Polizeidienststelle geschickt werden, die auf einem Fingerabdruckblatt die Abdrucke aller 10 Finger aufnimmt. Das Fingerabdruckblatt wird zum Teil unmittelbar, zum Teil über das Bundesamt in Zirndorf an das Bundeskriminalamt versandt.

Datei daktyloskopische Daten des Bundeskriminalamts

Im Bundeskriminalamt werden die Zehn-Finger-Abdrucke unter Verwendung des sog. Kurzsatzes verformelt. Die Formel und eine sog. Verknüpfungsnummer werden in die Datei daktyloskopische Daten eingespeichert. In dieser Datei sind alle vom Bundeskriminalamt und den Landeskriminalämtern ausgewerteten Fingerabdruckformeln enthalten, die aus der ED-Behandlung in Straf-, Asyl- und Ausländerverfahren gewonnen worden sind. Das Bundeskriminalamt und die Landeskriminalämter können in diese Datei Daten eingeben und abfragen.

ED-Datei des Bundeskriminalamts

Personendaten der Asylbewerber, deren Fingerabdruckblätter an das Bundeskriminalamt übersandt wurden, werden in einer sog. ED-Datei gespeichert. Dieser Datenbestand ist Teil des bundesweiten Informationssystems der Polizei (INPOL) und kann von jeder Polizeidienststelle mit INPOL-Anschluß abgefragt werden.

Die gegen die Speicherung beim BKA erhobenen rechtlichen Bedenken sind unbegründet, da § 13 Abs. 3 AsylVfG ausdrücklich vorsieht, daß das BKA dem Bundesamt in Zirndorf bei der Auswertung der

erkennungsdienstlichen Unterlagen Amtshilfe leistet. Nur wenn die Unterlagen zentral gespeichert werden, können neu eingehende Fingerabdrucke mit vorhandenen beim BKA verglichen werden und so der mit der ED-Behandlung verfolgte Zweck erreicht werden. Im übrigen geht § 13 Abs. 3 AsylVfG eindeutig von einer Speicherung durch das BKA aus.

Zehn-Finger- oder Ein-Finger-Abdruck

Unter dem Gesichtspunkt des Übermaßverbots ist überlegt worden, ob durch den Zehn-Finger-Abdruck ein Übermaß an Daten erhoben und gespeichert würde und statt dessen der Abdruck eines Fingers genüge.
Für die hinreichend zuverlässige Bestimmung der Identität eines Menschen durch das Fingerabdruckverfahren gibt es nach den Regeln der Daktyloskopie zwei Verfahren
- die Kurzverformelung aller Zehn-Finger-Abdrukke oder
- die umfassendere Verformelung jeweils eines einzigen Fingerabdrucks.

Das Bundeskriminalamt hat sich für die Kurzverformelung aller Zehn-Finger-Abdrucke entschieden, weil eine Kurzverformelung weniger zeitaufwendig ist. Diese Entscheidung obliegt der Kontrolle des Bundesbeauftragten für den Datenschutz. Solange das Bundeskriminalamt an der Kurzverformelung aller Zehn-Finger-Abdrucke festhält, haben die Landesbehörden von den Asylbewerbern die Abdrucke aller 10 Finger zu nehmen.

10. Steuerverwaltung

10.1 Änderungen im Datenschutzrecht für die Steuerverwaltung

Seit mehreren Jahren werden von den Finanzministerien des Bundes und der Länder Überlegungen zur Novellierung der Abgabenordnung (AO) angestellt. Die AO enthält die wesentlichen Vorschriften für das Besteuerungsverfahren, darunter auch Regelungen mit Datenschutzbezug, z. B. in § 30 das Steuergeheimnis, das Datenübermittlungen durch Steuerbehörden betrifft. Die wichtigsten Punkte der vorgesehenen Änderungen der AO sind aus der Sicht des Datenschutzes:

- die **Anwendung von Bundes- oder Landesdatenschutzrecht** für Steuerbehörden

  Soweit in der AO nicht besondere Vorschriften die Datenverarbeitung regeln (z. B. Steuergeheimnis), wird voraussichtlich das materielle Datenschutzrecht nach dem BDSG anzuwenden sein. Soweit bisher erkennbar, werden sich dagegen die Datenschutzkontrolle der Steuerbehörden und die sonstigen Mitwirkungsrechte der Datenschutzbeauftragten im wesentlichen nach Landesdatenschutzrecht richten.

  Für die gemeindlichen Steuerverwaltungen wird voraussichtlich das Bayerische Datenschutzgesetz auch materiell gültig bleiben, damit nicht Bundes- und Landesrecht nebeneinander angewendet werden müssen, was insbesondere bei kleineren Gemeindeverwaltungen zu Schwierigkeiten führen könnte.

  Ob das BDSG durch Aufnahme aller relevanten Datenschutzvorschriften in die AO vollständig ersetzt wird, ist nicht bekannt. Gegen eine Änderung der AO in der geschilderten Art habe ich keine Einwände erhoben. Ich gehe dabei allerdings davon aus, daß sich die Besonderheiten des Kontrollverfahrens und der Mitwirkungsrechte nach dem Bayerischen Datenschutzgesetz richten (z. B. Unterrichtung des Datenschutzbeirats über Beanstandungen).

- die Nutzung von Adreßdaten aus der gemeindlichen Grundsteuerdatei durch die Gemeinde

  Die Nutzung der Adressen von Grundstückseigentümern aus der gemeindlichen Grundsteuerdatei soll zur Verwaltung anderer **grundstücksbezogener** Abgaben möglich sein. Mein Vorschlag, die Nutzung der Anschriften auch für andere öffentliche Aufgaben der Gemeinden zuzulassen, da es sich um wenig sensible Daten handelt, scheint jedoch nicht berücksichtigt zu werden.

  Dies hätte allerdings zur Folge, daß die bisherige **Praxis von vielen Gemeinden**, die Adreßdaten aus der Grundsteuerdatei auch für andere gemeindliche Aufgaben heranzuziehen, beendet werden müßte. Bei Kontrollen müßte ich die Nutzung von Adreßdaten aus den Grundsteuerdateien für andere öffentliche Aufgaben künftig beanstanden.

- die Bekanntgabe der Grundsteuermeßbescheide an Gemeinden

  Wie bereits in meinem letzten Tätigkeitsbericht (Nr. 9.4) ausgeführt, halte ich die Übersendung der kompletten Gewerbesteuermeßbescheide an Gemeinden zur Festsetzung der Gewerbesteuer in vielen Fällen nicht für erforderlich. Da der Bayerische Staatsminister der Finanzen meiner Meinung grundsätzlich zugestimmt hat, sollte im Zuge der AO-Novellierung auch die einschlägige Vorschrift des § 184 Abs. 3 AO entsprechend geändert werden.

10.2 Bundesverfassungsgericht: Besteuerung von Kapitaleinkünften

Das Urteil des Bundesverfassungsgerichts vom 25.7.1991 (Zins-Urteil) enthält bedeutsame Ausführungen über die rechtlichen Möglichkeiten des Gesetzgebers, die Erhebung personenbezogener Daten

für Steuerzwecke vorzusehen. Nach dem Urteil seien **steuerliche Kontrollmitteilungen** und **Auskunftspflichten** mit Grundrechten der Banken und der Bankkunden vereinbar. Dies gelte auch unter dem Aspekt des grundrechtlichen Datenschutzes.

Zwar lasse der **Bankenerlaß** trotz des von ihm betonten Vertrauensverhältnisses zwischen Kreditinstitut und Kunden die Einzelauskunftspflicht der Kreditinstitute nach den § 93 ff AO rechtlich unberührt; dessen ungeachtet schaffe er nach dem Gesamtinhalt seiner Regelungen ein Klima der Zurückhaltung und des Zögerns, das eine zuverlässige Ermittlung der Kapitaleinkünfte prinzipiell verhindere. Der Bankenerlaß habe dazu beigetragen, die steuerlichen Ermittlungsmöglichkeiten nicht voll auszuschöpfen, indem er die Rücksichtnahme auf das besondere Vertrauensverhältnis zwischen Kreditinstitut und Kunden sowie ein generelles Vertrauen in die Vollständigkeit und Richtigkeit der Steuererklärung vorsehe.

Diese Beschränkungen seien jedoch verfassungsrechtlich nicht geboten. Steuerliche Kontrollmitteilungen und Auskunftspflichten dürften vielmehr **im überwiegenden Interesse der Allgemeinheit** unter Beachtung des Grundsatzes der Verhältnismäßigkeit durch Gesetz vorgesehen werden. Die bisher im Steuerrecht verankerten Auskunfts- und Anzeigepflichten sowie die Ermächtigung zur Ausschreibung von Kontrollmitteilungen genügten diesen Voraussetzungen. Sie seien gesetzlich hinreichend bestimmt und entsprächen dem Grundsatz der Verhältnismäßigkeit.

Darüber hinaus ist datenschutzrechtlich von allgemeinem Interesse, daß das Bundesverfassungsgericht ausdrücklich offen läßt, „ob der Informationszugriff auf privates Finanzkapital und seine Erträge als Vorgang des marktoffenbaren Erwerbs **ohne besonderen persönlichkeitsgeprägten Gehalt** überhaupt vom Gewährleistungsinhalt des verfassungsrechtlichen Datenschutzes erfaßt wird".

Hier weist das Bundesverfassungsgericht darauf hin, daß nur Daten mit einem gewissen **Mindestmaß an Bezug** zu einer bestimmten natürlichen Person vom Grundrecht der informationellen Selbstbestimmung erfaßt werden. Da es auf diesen Gesichtspunkt für die Entscheidung aber nicht weiter ankam, brauchte das Gericht auf seine wichtigen früheren Ausführungen zur Bedeutung des Verwendungszusammenhanges nicht einzugehen (z. B. im Volkszählungsurteil). Gleichwohl machen die zitierten Ausführungen bewußt, daß Angaben desto weniger dem verfassungsrechtlichen Datenschutz unterliegen, je schwächer der **Bezug zur Privatsphäre einer natürlichen Person** ausgeprägt ist.

Wenn das Gericht in der Begründung allerdings ausführt, daß mit der gesetzlichen Ausgestaltung des Steuergeheimnisses der Gesetzgeber hinreichende Sicherheitsvorkehrungen gegen eine mißbräuchliche Verwendung der Angaben getroffen habe und daß die Regelungen der §§ 30, 31 AO i.V.m. § 355 StGB das unbefugte Offenbaren oder Verwerten der Angaben des Auskunftspflichtigen ausschlössen, so kann dies sicherlich nur bedeuten, daß der Gesetzgeber selbst insoweit getan hat, was ihm oblag. Technisch-organisatorische Datensicherung wird dadurch keinesfalls überflüssig.

Das Bundesverfassungsgericht betont in seinem Urteil das **Verifikationsprinzip**. Dies schließt jedoch nicht aus, daß nicht gleichwohl nach dem Verhältnismäßigkeitsgrundsatz aus verschiedenen Möglichkeiten der Verifikation von Angaben Steuerpflichtiger dasjenige Verfahren zu wählen ist, das den geringstmöglichen Eingriff darstellt.

10.3 Prüfung bei einem Finanzamt

Im Juni 1991 wurde bei einem Finanzamt eine datenschutzrechtliche Prüfung durchgeführt. Die Kontrollbefugnis des Landesbeauftragten ergibt sich seit 1. Juni 1991 aus Art. 28 BayDSG, § 24 Abs. 2, 4 bis 6 BDSG. Gegenstand der Kontrolle waren **Dateien, Karteien** und **ausgewählte Aktenunterlagen**. Kontrollzweck der Überprüfung von Steuerakten war die Feststellung von **Datenübermittlungen** an Dritte durch das Finanzamt aus Dateien des Finanzamts. Außerdem wurde in Dateien und Karteien die Erforderlichkeit der gespeicherten Informationen überprüft. Ein weiterer Prüfungspunkt war die organisatorische und rechtliche **Abschottung** des Finanzamts gegenüber einer dort eingerichteten Außenstelle eines anderen Finanzamts.

Die datenschutzrechtliche Überprüfung hat nur geringe Mängel ergeben:

- Bei der Betriebskartei der **Betriebsprüfungsstelle** wurde festgestellt, daß die Löschung von Hinweisen nach Wegfall ihrer Erforderlichkeit zur Aufgabenerfüllung nicht geregelt war. Die Einführung eines Löschungsverfahrens wurde gefordert.

- Die Hopfengestehungskosten werden bisher aufgrund freiwilliger Mitarbeit der Hopfenerzeuger ermittelt. Die ausgefüllten Formulare zur Kostenerfassung wurden seither mit identifizierenden Daten der Hopfenerzeuger an die Oberfinanzdirektion München weitergeleitet, obwohl die Oberfinanzdirektion nach eigenen Angaben keine identifizierenden Merkmale benötigt. Die **Anonymisierung der Formulare** wurde gefordert.

- Die Kfz-Steuerstelle des Finanzamts erhielt von der zuständigen Straßenverkehrsbehörde Kopien von Taxi-Genehmigungen. Diese Datenübermittlungen wurden inzwischen eingestellt, weil sie zur Aufgabenerfüllung des Finanzamts nicht erforderlich sind.

In Karteien der **Personalstelle** des Finanzamts sind einige Informationen mangels Erforderlichkeit zu löschen bzw. nicht mehr zu erheben:

- In der **Krankheitskartei** sind in vielen Fällen Angaben über die Art der Erkrankung enthalten, welche die Bediensteten nach Aussage des Finanzamts selbst gegeben haben. Gezielte Fragen nach Art der Erkrankung würden nicht gestellt. Grundsätzlich sind diese Angaben in der Kartei zur Aufgabenerfüllung des Amtes nicht notwendig. Das Finanzamt wurde aufgefordert, Angaben über die Art der Erkrankung nur noch dann einzutragen, wenn Bedienstete dies ausdrücklich wünschen, z. B. aus Gründen dienstlicher Verwendbarkeit.
- Die **Personalkarteikarten** sehen derzeit mehr Angaben vor, als zur Aufgabenerfüllung erforderlich sind (z. B. Beruf, Religionsgemeinschaft und Geburtsname des Ehegatten, Flüchtling, Betroffener nach Art. 131 GG). Auf die Eintragung solcher nicht benötigter Angaben muß — wie teilweise schon geschehen — verzichtet werden. Beim Neudruck der Karteikarten ist die Erforderlichkeit für jedes Datenfeld zu überprüfen.

Eine **Datenübermittlung** des Finanzamts an Dritte außerhalb einer Betriebsprüfung, die nur in Akten hätte festgestellt werden können, wurde bei der stichprobenweisen Aktendurchsicht nicht festgestellt. Bei dieser Gelegenheit fand sich jedoch die Mitteilung einer anderen staatlichen Dienststelle über eine Zahlung an einen Steuerpflichtigen. Die Überprüfung dieses Vorgangs bei der datenübermittelnden Behörde hat inzwischen ergeben, daß dort die schriftliche Zustimmung des Betroffenen zur Datenübermittlung an das Finanzamt vorlag.

Die Überprüfung der **Abschottung** des Finanzamts gegenüber der dort untergebrachten Außenstelle eines anderen Finanzamts ergab keine Mängel. Die Außenstelle verfügt in allen Bereichen über eigene Einrichtungen (z. B. eigene Diensträume mit gesonderter Schließanlage, eigenes DV-Subsystem, eigener Registraturraum) sowie eigenes Personal. Zugriff auf die Aktenunterlagen und auf die gespeicherten Daten der Außenstelle haben nur deren Mitarbeiter. Das gastgebende Finanzamt hat alle notwendigen Vorkehrungen getroffen, damit Steuerdaten der Außenstelle nicht unbefugt zur Kenntnis genommen werden können.

10.4 Neue Lohnsteuerkarte bei Arbeitgeberwechsel

Im Berichtszeitraum haben sich Bürger wiederholt darüber beklagt, daß sie dem neuen Arbeitgeber ihre bisherigen Einkünfte aus nichtselbständiger Tätigkeit durch Vorlage der (alten) Lohnsteuerkarte offenbaren müßten. Sie sehen dadurch ihr Recht auf informationelle Selbstbestimmung ohne Notwendigkeit eingeschränkt.

In seiner Stellungnahme kündigte das Finanzministerium an, daß sich die Lohnsteuer-Referenten des Bundes und der Länder dieses Problems „bei nächster Gelegenheit" annehmen würden. Ein Ergebnis liegt noch nicht vor.

Das Einkommensteuergesetz (EStG) gestattet für Fälle des Arbeitsplatzwechsels derzeit die Ausstellung einer neuen Lohnsteuerkarte nicht. Die Steuerverwaltung sieht im Falle des Arbeitsplatzwechsels nur bei Vorlage der alten Lohnsteuerkarte die korrekte Einbehaltung der Lohnsteuer gewährleistet. Nach meiner Auffassung könnte jedoch durch geeignete Maßnahmen, z.B. durch eine besondere Kennzeichnung der neuen Lohnsteuerkarte, Abgabe der ersten Lohnsteuerkarte an die Steuerbehörde zur späteren Vornahme einer Arbeitnehmerveranlagung u.ä., sichergestellt werden, daß nicht zu wenig Lohnsteuer einbehalten oder zuviel erstattet würde (§§ 39 b Abs. 3, 42ff EStG).

Im Hinblick auf das informationelle Selbstbestimmungsrecht sollte es der Entscheidung des Arbeitnehmers überlassen bleiben, ob er dem neuen Arbeitgeber seine bisherigen Einkünfte offenbart. Das Steuerrecht muß hierzu die notwendigen Voraussetzungen schaffen.

11. Vermessungswesen

11.1 Automatisiertes Liegenschaftsbuch (ALB)

Das von den staatlichen Vermessungsämtern zu führende Liegenschaftskataster hat die Aufgabe, die Liegenschaften des Staatsgebiets, d.h. die Grundstücke und Gebäude, im Katasterkartenwerk darzustellen und in Katasterbüchern zu beschreiben. Rechtliche Grundlage dieser Datenverarbeitung ist Art. 6 des Bayer. Vermessungs- und Katastergesetzes. Um der Fülle dieser Daten Herr zu werden und um diese ständig auf dem neuesten Stand zu halten, wurde in den letzten Jahren ein automatisiertes Datenverarbeitungsverfahren entwickelt, das von allen Vermessungsämtern eingesetzt wird. Gegenstand von Erörterungen im Berichtszeitraum waren die Datenübermittlung an die **Landkreise** und die Nutzung der Daten des Liegenschaftsbuches sowie die **Aufnahme von zusätzlichen öffentlich-rechtlichen Daten** auf Antrag von Gemeinden in das Automatisierte Liegenschaftsbuch.

11.1.1 Einsicht und Auskunft

Die Zulässigkeit der Übermittlung von personenbezogenen Daten aus dem Automatisierten Liegenschaftsbuch richtet sich nach Art. 11 des Vermessungs- und Katastergesetzes. Danach wird jedem, der ein berechtigtes Interesse darlegt, **Einsicht** in die Karten und Bücher des Liegenschaftskatasters gewährt und **Auskunft** aus dem Liegenschaftskataster erteilt,

soweit nicht Interessen des öffentlichen Wohls entgegenstehen.

Gemeinden haben zur Wahrnehmung ihrer kommunalen Aufgaben grundsätzlich ein berechtigtes Interesse an den ALB-Daten für alle Flurstücke im Gemeindegebiet. Schon bisher erhielten sie auf Antrag eine Zweitschrift des Liegenschaftsbuches, das sogenannte Sekundärkataster. Nach Umstellung des Liegenschaftsbuches auf das Automatisierte Liegenschaftsbuch werden die ALB-Daten für ein Gemeindegebiet auf der Grundlage einer **Vereinbarung** über die Nutzung des Automatisierten Liegenschaftsbuches zwischen dem staatlichen Vermessungsamt und der jeweiligen Gemeinde abgegeben. Die Rechte und Pflichten der Gemeinde, insbesondere auch die Einhaltung des Datenschutzes, sind detailliert in der mit mir abgestimmten Vereinbarung niedergelegt. Ich hatte die Aufnahme der Verpflichtung der Gemeinde gefordert, auch innerhalb der Gemeinde die personenbezogenen Daten des ALB nur denjenigen Stellen zur Verfügung zu stellen, die sie zur rechtmäßigen Erfüllung der ihnen zugewiesenen Aufgaben benötigen (Art. 17 Abs. 3 BayDSG).

Mit dem Staatsministerium der Finanzen und Vertretern des Landkreistages habe ich geprüft, ob es zulässig ist, auch an die **Landkreise** regelmäßig ALB-Daten für alle im Landkreisgebiet gelegenen Gründstücke zu übermitteln. Zwar kann auch Landkreisen nach Art. 11 Vermessungs- und Katastergesetz Einsicht in die Karten und Bücher des Liegenschaftskatasters gewährt und Auskunft aus dem Liegenschaftskataster erteilt werden, wenn die Wahrnehmung einer konkreten Aufgabe ein berechtigtes Interesse begründet. Ich habe jedoch Zweifel geäußert, ob für die Übermittlung sämtlicher Daten des ALB für alle im Landkreisgebiet gelegenen Grundstücke ein berechtigtes Interesse besteht, da eine Notwendigkeit für diese umfassende Datenübermittlung zur Wahrnehmung von Landkreisaufgaben — von Ausnahmen abgesehen — nicht erkennbar ist. Bei der Weitergabe sämtlicher Daten des Automatisierten Liegenschaftsbuches an die Landkreise würde es sich vielmehr um eine unzulässige Datenverarbeitung auf Vorrat handeln, um eine möglicherweise künftig sich ergebende Aufgabe des Landkreises wahrnehmen zu können oder um die Daten zur Weitergabe an kreisangehörige Gemeinden bereitzuhalten. Anders als bei den Gemeinden, bei denen wegen ihres allseitigen Wirkungskreises (Art. 6 Gemeindeordnung) stets ein berechtigtes Interesse an der Übermittlung der Daten sämtlicher Grundstücke des Gemeindegebiets angenommen werden kann, hat der Landkreis keine allumfassende Kompetenz zur Regelung der örtlichen Angelegenheiten.

11.1.2 Zusätzliche Daten

Die Mustervereinbarung zwischen Vermessungsverwaltung und Gemeinden über die Nutzung des Automatisierten Liegenschaftsbuches sah auch vor, daß auf Antrag der Gemeinde sogenannte **zusätzliche öffentlich-rechtliche Daten** nachrichtlich als Hinweise in das ALB übernommen und auf der Grundlage der von der Gemeinde gemeldeten Daten auf dem laufenden gehalten werden. Bei diesen Daten handelt es sich um nachrichtliche Hinweise, die das Grundstück betreffen, wie zum Beispiel Hinweise zum Naturschutz, auf Biotope, Denkmäler usw. Diese Datenverarbeitung würde erfolgen im Interesse und auf Veranlassung der Kommune, nicht jedoch zur Aufgabenerfüllung der Vermessungsämter. Ich habe darauf hingewiesen, daß für die Speicherung dieser zusätzlichen öffentlich-rechtlichen Daten keine gesetzliche Grundlage bestehe, insbesondere das Vermessungs- und Katastergesetz nicht die erforderliche Rechtsgrundlage darstelle. Der Inhalt des Liegenschaftskatasters ist in den Art. 5 bis 11 Vermessungs- und Katastergesetz abschließend festgelegt; derartige nachrichtliche Hinweise sind nicht vorgesehen. Zwischenzeitlich wurde die Möglichkeit der Übernahme zusätzlicher öffentlich-rechtlicher Daten in das ALB in der Mustervereinbarung gestrichen.

11.1.3 Gesamtkonzept

Nach meiner Auffassung sollte die Frage der Übermittlung von Daten des ALB an Landkreise sowie eines möglichen Datenaustausches zwischen Gemeinden und Landkreisen nicht losgelöst von einem **Gesamtkonzept** über eine Verarbeitung von Grundstücksdaten durch Landkreise und Gemeinden beurteilt werden. In diesem Gesamtkonzept ist auch die Aufnahme von zusätzlichen öffentlich-rechtlichen Daten auf Antrag der Gemeinden in das ALB zu regeln. Das geltende Vermessungs- und Katastergesetz kann hierfür keine Rechtsgrundlage sein. Die Notwendigkeit eines Gesamtkonzepts ergibt sich noch deutlicher, falls künftig die Schaffung eines umfassenden öffentlichen **Grundstücksinformationssystems** geplant würde.

Das Staatsministerium der Finanzen und der Landkreistag teilen meine Auffassung. Die Vereinbarung über die Nutzung des Automatisierten Liegenschaftsbuches zwischen dem Vermessungsamt und Gemeinden ist auf Landkreise nicht übertragbar. Die Landkreise erhalten deshalb im Gegensatz zu Gemeinden nicht regelmäßig alle Daten sämtlicher Flurstücke im Landkreis, sondern nur im Einzelfall bei Vorliegen eines berechtigten Interesses.

11.2 Prüfung eines Vermessungsamts

Bei der Kontrolle eines Vermessungsamts habe ich die Gewährung von Einsicht in die Karten und Bücher des Liegenschaftskatasters sowie die Erteilung

von Auskünften hieraus überprüft. Ich habe dabei festgestellt, daß mündliche oder telefonische **Anfragen von Privatpersonen** in mündlicher Form, schriftliche Anfragen in Schriftform beantwortet werden. Die Mitarbeiter des Vermessungsamts sind angewiesen, in jedem Fall zu prüfen, aus welchem Grunde Einsicht oder Auskunft verlangt wird und ob ein berechtigtes Interesse vorliegt. Bei Zweifeln am Vorliegen eines berechtigten Interesses wird der Anfragende an den Behördenleiter verwiesen, der über die Auskunftserteilung entscheidet. Schriftliche Anweisungen des Behördenleiters an die Bediensteten zur Beurteilung des berechtigten Interesses und zur Durchführung der Auskunftserteilung bestehen nicht.

Bei mündlichen Auskünften erfolgt weder eine schriftliche Dokumentation von Inhalt und Begründung der Anfrage noch über die Prüfung des Antrags und die erteilte Auskunft. Es ist somit später nicht mehr nachvollziehbar, wer sich mit welchem Auskunftsbegehren an das Vermessungsamt gewandt hat und aus welchem Grunde welche Auskunft erteilt wurde. Bei schriftlichen Anfragen verbleibt zwar das Schreiben für 10 Jahre in der sog. Antragssammlung des Vermessungsamts. Ein Nachweis über die schriftliche Auskunft an den Anfragenden (z.B. Durchschrift) wird dagegen nicht aufbewahrt. Somit kann auch in diesem Fall die Auskunftserteilung nicht nachvollzogen und überprüft werden.

Nach Art. 11 Abs. 1 des Bayerischen Gesetzes über die Landesvermessung und das Liegenschaftskataster (VermKatG) wird nur demjenigen, der ein **berechtigtes Interesse** darlegt, Einsicht in die Karten und Bücher des Liegenschaftskatasters gewährt und Auskunft aus dem Liegenschaftskataster erteilt, soweit nicht Interessen des öffentlichen Wohls entgegenstehen. Da das Liegenschaftskataster neben den Daten der Grundstücke, wie z.B. Gestalt, Lage und Größe der Liegenschaften, auch Daten der Eigentümer und Inhaber von Erbbaurechten enthält, besteht ein schützenswertes Interesse der Betroffenen, daß nicht jedermann Einblick in das Kataster erhält. Der Schutz dieses Interesses ist nur dann ausreichend gewährleistet, wenn Anfrage und Auskunft beim Vermessungsamt dokumentiert werden und so eine Kontrolle möglich ist (vgl. auch Ziff. 7.11).

12. Personalwesen

12.1 Mitbestimmung des Personalrates

Im Berichtsjahr habe ich in einigen Fällen Behörden auf das Mitbestimmungsrecht des Personalrates gem. Art. 75 a Abs. 1 Nr. 1 BayPVG hingewiesen. Danach hat der Personalrat bei der Einführung und Anwendung technischer Einrichtungen zur **Überwachung des Verhaltens oder der Leistung** der Beschäftigten mitzubestimmen. Die Behörden hatten geltend gemacht, sie hätten nicht die Absicht, die Bediensteten mit den technischen Einrichtungen zu überwachen. Auf eine solche Absicht kommt es jedoch nicht an. Nach herrschender Rechtsprechung genügt für die Anwendbarkeit dieser Vorschrift bereits die **objektive Eignung** zur Überwachung.

12.2 Grundsätze zum Datenschutz der Arbeitnehmer im öffentlichen Dienst

Die Datenschutzbeauftragten der Länder und des Bundes haben in ihrer Konferenz am 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes Grundsätze zum Datenschutz der Arbeitnehmer im öffentlichen Dienst beschlossen. Der Text ist in der Anlage zu diesem Tätigkeitsbericht abgedruckt. Diese Grundsätze sollten bei der weiteren Ausgestaltung des Dienstrechts beachtet werden.

12.3 Telefongesprächsdatenerfassung

Bereits im 8. Tätigkeitsbericht (Nr. 9.3) habe ich das Thema „Telefongesprächsdatenerfassung" ausführlich behandelt. Das Innenministerium hat im April 1991 für den erstmaligen Einsatz automatisierter Verfahren, mit denen Telefongesprächsdaten verarbeitet werden (sog. Gebührencomputer) für seinen Bereich eine generelle datenschutzrechtliche Freigabe erteilt. Die dort genannten Voraussetzungen entsprechen größtenteils den Grundsätzen, die das Staatsministerium der Finanzen Mitte 1986 zur Wahrung der Belange des Datenschutzes bekanntgegeben hat.

Darüber hinaus trifft das Innenministerium jedoch zwei datenschutzrechtlich bedeutsame Festlegungen:

1. Personalvertretungen

   Daten von dienstlichen Gesprächen der Personalvertretungen dürfen ohne Zustimmung der betroffenen Bediensteten nur **summarisch** (Summe der Gebühreneinheiten je Nebenstelle) ausgewertet werden.

2. Bedienstete, die einer besonderen Schweigepflicht unterliegen

   Bei Behördenbediensteten, die im Rahmen einer **freiwilligen** Beratung (z.B. nach Art. 11 Abs. 1 GDG), insbesondere

   - in der Beratung Drogensüchtiger, psychisch Kranker oder Behinderter,
   - in der Ehe- und Familienberatung,
   - in der gesundheitlichen Beratung von Menschen, die an einer übertragbaren Krankheit leiden,

   tätig sind, darf eine Auswertung der gespeicherten Daten ohne deren Zustimmung ebenfalls nur summarisch vorgenommen werden.

   Auf meine Anregung hin wird den Behörden im Bereich des Staatsministeriums des Innern emp-

fohlen, diesem Personenkreis einen Anschluß zur Verfügung zu stellen, bei dem sogar auf eine **Speicherung der Zielnummer verzichtet** wird. Hierfür sollte der regionale Bereich in dem Ferngespräche geführt werden können, beschränkt werden (z.B. auf den Orts- und Nahbereich, sowie — über Kurzwahlnummern — auf wichtige Anschlüsse, mit denen häufig dienstlich gesprochen wird).

12.4 Eigene Rechtsstellung für Angehörige im Beihilfeverfahren

Nach dem geltenden Beihilferecht müssen berücksichtigungsfähige Angehörige von öffentlichen Bediensteten ihre Belege über beihilfefähige Leistungen (Arzt- und Apothekenrechnungen) dem Beihilfeberechtigten überlassen. Dadurch werden ihm Angaben zu gesundheitlichen Problemen bekannt, die er sonst möglicherweise nicht erfahren würde, wie z.B. psychotherapeutische Behandlungen oder andere hochsensible Krankheitsdiagnosen. Dies kann vor allem in abgekühlten Partnerschafts- oder Eltern-Kind-Beziehungen Probleme aufwerfen. Einige Landesdatenschutzbeauftragte fordern daher in jüngster Zeit einen eigenen Beihilfeanspruch für volljährige Angehörige der Bediensteten im öffentlichen Dienst. Das Staatsministerium der Finanzen hat statt dessen folgende Lösungsansätze vorgeschlagen:

- Getrennte Übersendung von Antrag durch den Bediensteten und Belegen durch den Angehörigen oder
- Unterschreiben des Beihilfeantrags durch einen Angehörigen „in Vertretung" für den Beihilfeberechtigten. Der Beihilfeberechtigte könnte die Beihilfestelle gleichzeitig darüber in Kenntnis setzen, daß mit dem Eingang eines derartigen Antrags zu rechnen sei und um Rücksendung an den Angehörigen bitten, oder
- in kritischen Zweifelsfällen: Übergabe des unterschriebenen Beihilfeantragsformulars an den Angehörigen, der es zusammen mit den Arztrechnungen und Rezepten an die Beihilfestelle senden und die Abrechnung von dort unmittelbar erhalten könne.

Eine Kenntnisnahme des Beihilfeberechtigten vom Inhalt der Arztrechnungen und Rezepte seiner Angehörigen könnte auf diese Weise vermieden werden.

Die Datenschutzkonferenz hat sich am 26./27. September 1991 für einen eigenständigen Beihilfeanspruch volljähriger Angehöriger ausgesprochen.

12.5 Verarbeitung personenbezogener Personaldaten durch Gewerbeaufsichtsämter

Mit dem Staatsministerium für Arbeit, Familie und Sozialordnung habe ich die Frage erörtert, ob Gewerbeaufsichtsämter im automatisierten Verfahren eine Übersicht über die von den einzelnen Gewerbeaufsichtsbeamten durchgeführten Dienstgeschäfte („personenbezogene Beamtenliste") erstellen dürfen. Der Hauptpersonalrat äußerte die Befürchtung, daß die personenbezogene Sammlung der Daten dem Amtsleiter eine unverhältnismäßige Überwachungsmöglichkeit einräume. Für die Steuerung und Beurteilung der Mitarbeiter seien andere geeignete Instrumente (die manuell geführten Tagebücher) vorhanden. In Übereinstimmung mit dem Ministerium vertrete ich folgende Auffassung:

1. Die **beamtenbezogene Erfassung der Dienstgeschäfte** der einzelnen Beamten ist für den Amtsleiter der Gewerbeaufsichtsämter zur Wahrnehmung seiner Dienst- und Fachaufsicht erforderlich. Die aus einem Teil der Tagebucheintragungen automatisiert erstellte personenbezogene Beamtenliste stellt ein geeignetes und angemessenes Mittel dar, um einen Überblick über leistungsbezogene Daten der Mitarbeiter zu gewinnen.

   Andere geeignete Instrumente, die dem Amtsleiter einen schnellen **quantitativen** Überblick gewähren, sind nicht ersichtlich. Insbesondere ist der Verweis auf die in den Tagebüchern enthaltenen Informationen über die durchgeführten Betriebsbesichtigungen in vielen Fällen keine angemessene Alternative. Für den Amtsleiter muß die Möglichkeit bestehen, kurzfristig quantitativ leistungsbezogene Daten seiner Mitarbeiter abzurufen, um auch eventuellen Vollzugsdefiziten schnell Rechnung tragen zu können. Die Erfüllung dieser Aufgabe im Rahmen der Dienst- und Fachaufsicht ist nicht gewährleistet, wenn anstelle der Beamtenliste jeweils eine manuelle Auswertung der umfangreichen Tagebücher erfolgen müßte.

2. Die beamtenbezogene Erfassung der Dienstgeschäfte birgt allerdings das Risiko, daß die Mitarbeiter nur anhand der Beamtenliste beurteilt werden, die lediglich zur Quantität, nicht aber zur Qualität der Arbeit hinreichend signifikante Aussagen erlaubt. Ich habe daher angeregt, eine Dienstvereinbarung auszuarbeiten, die einen derartigen Eingriff in schutzwürdige Belange der Bediensteten ausschließt. Die Vereinbarung sollte sicherstellen, daß bei Beurteilungen zuverlässig auch die sonstigen zur Beurteilung der Qualität der Arbeit maßgeblichen Informationen berücksichtigt werden.

12.6 Informationspflicht des örtlichen Personalrats gegenüber dem Vertrauensmann der Schwerbehinderten

Ein Mitglied eines Personalrates fragte an, ob der Vertrauensmann der Schwerbehinderten in seiner Eigenschaft als Schwerbehindertenvertreter von allen mitwirkungs- und mitbestimmungspflichtigen Angelegenheiten des Personalrats Kenntnis erhalten müsse. Da der Vertrauensmann der Schwerbehinderten kein gewähltes Mitglied des Personalrates sei, dürfe

er nur bei solchen Maßnahmen beteiligt werden, bei denen Belange der Schwerbehinderten angesprochen werden.

In Übereinstimmung mit dem Staatsministerium der Finanzen vertrete ich hierzu folgende Auffassung:

- Nach Art. 40 Abs. 1 BayPVG hat die Schwerbehindertenvertretung das Recht, an allen Sitzungen des Personalrats und seiner Ausschüsse beratend teilzunehmen. Dabei ergibt sich aus dem Wortlaut („alle Sitzungen") sowie aus Sinn und Zweck der Vorschrift, daß eine Beschränkung auf Sitzungen, in denen Belange der Schwerbehinderten angesprochen werden, **nicht** vorgesehen ist. Nach der Vorstellung des Gesetzgebers sollte der Schwerbehindertenvertretung das Recht zustehen, dem Personalrat beratend zur Seite zu stehen, falls sich in den Personalratssitzungen spezifische Interessen der schwerbehinderten Beschäftigten abzeichnen.

- Demgegenüber fehlt der Schwerbehindertenvertretung die durch Wahlen bekräftigte Legitimation, um die Interessen aller Beschäftigten wahrzunehmen. Der Vertrauensperson der Schwerbehinderten kann daher nicht das Recht zugestanden werden, über **alle mitwirkungs- und mitbestimmungspflichtigen Angelegenheiten des Personalrats** informiert zu werden. Infolgedessen stehen die gesetzlich festgelegten Rechte (z.B. Stimmrecht gem. Art. 40 Abs. 2 BayPVG, Vetorecht nach § 25 Abs. 4 S. 2 Schwerbehindertengesetz) der Schwerbehindertenvertretung nur dann zu, soweit Beschlüsse überwiegend Schwerbehinderte betreffen. Handelt es sich um Angelegenheiten, die einzelne schwerbehinderte Beschäftigte oder die schwerbehinderten Beschäftigten als Gruppe betreffen, kann die Schwerbehindertenvertretung nach Art. 34 Abs. 3 BayPVG beantragen, eine Personalratssitzung anzuberaumen und den Gegenstand auf die Tagesordnung zu setzen. In allen anderen Angelegenheiten steht der Schwerbehindertenvertretung nur das Recht der Teilnahme an den Sitzungen gem. Art. 40 BayPVG zu.

- Die Vertrauensperson der Schwerbehinderten hat keinen Anspruch auf vorbereitende Unterlagen bzw. ergänzende Informationen zu Angelegenheiten, welche die Belange der Schwerbehinderten nicht berühren. In diesen Fällen stehen zusätzliche Informationsmittel nur den gewählten Personalratsmitgliedern zu.

- Gem. Art. 41 BayPVG ist über jede Verhandlung des Personalrats eine Niederschrift aufzunehmen. Während die Mitglieder des Personalrats einen vollständigen Abdruck der Niederschrift erhalten, ist der Schwerbehindertenvertretung nur der Teil der Niederschrift zuzuleiten, in dem Belange der Schwerbehinderten angesprochen sind.

12.7 Aufbewahrung polizeiärztlicher Gutachten

In einer Eingabe äußerte ein Polizeibeamter die Befürchtung, die Personalabteilung könnte in polizeiärztliche Unterlagen Einsicht genommen haben, die den **Personalakten** in einem verschlossenen und versiegelten Umschlag beiliegen. Nach einem Schreiben des Staatsministeriums des Innern vom 03.01.1979 darf dieser verschlossene Umschlag nur von den Polizeiärzten und deren ärztlichen Mitarbeitern geöffnet werden.

Bei anderen Beamten werden die Unterlagen über die amtsärztlichen Untersuchungen bei den **Amtsärzten**, d. h. den Gesundheitsämtern, aufbewahrt. Ich habe daher das Staatsministerium des Innern gebeten zu prüfen, ob die ärztlichen Unterlagen der Polizeibeamten mit vertretbarem Aufwand statt im Personalakt ähnlich wie bei anderen Beamten zentral beim **ärztlichen Dienst** aufbewahrt werden könnten.

Gleichzeitig habe ich gebeten zu prüfen, ob der Umschlag, in dem die Gesundheitsakten aufbewahrt werden, so gestaltet werden kann, daß eine **vollständige Übersicht** über stattgefundene Einsichtnahmen und über einsichtnehmende Personen entsteht. Gegenwärtig ergibt sich nämlich aus der Siegelmarke auf dem Umschlag nur, wer den Umschlag zuletzt verschlossen hat.

Den letzteren Vorschlag hat das Innenministerium sofort aufgegriffen. Eine vollständige Dokumentation über die Einsichtnahmen wird nun geführt. Die Aufbewahrung der amtsärztlichen Unterlagen beim medizinischen Dienst wurde jedoch abgelehnt, da dies die Nutzung der Unterlagen zu sehr erschwere. Die Unterlagen seien in dem gesonderten, verschlossenen und versiegelten Umschlag zuverlässig gegen Kenntnisnahme anderer Personen als der Polizeiärzte und ihrer Mitarbeiter geschützt.

Nach Einführung der vollständigen Dokumentation der Einsichtnahmen in den versiegelten Umschlag halte ich gegenwärtig die polizeiärztlichen Unterlagen für ausreichend gesichert.

13. Gewerbe und Handwerk

13.1 Datenschutzprüfung bei einer Handwerkskammer

Gegenstand der Prüfung einer Handwerkskammer waren die Formulare, mit denen Daten von Betroffenen erhoben werden, ferner die automatisierten Dateien und manuellen Karteien sowie die von der Kammer veranlaßten regelmäßigen Datenübermittlungen.

Der korrekten Gestaltung von Antragsformularen kommt besondere Bedeutung zu, weil sie für Art und Umfang der Datenerhebung und vielfach auch der

Datenverarbeitung maßgeblich sind. Bei einer Reihe von **Antragsformularen** fehlte der nach Art. 16 Abs. 2 BayDSG vorgeschriebene Hinweis darauf, ob der Betroffene zu den Angaben verpflichtet ist oder ob sie freiwillig sind. Außerdem war in etlichen Fällen fraglich, ob die Angaben zur Aufgabenerfüllung erforderlich sind (vgl. auch Nr. 13.2).

Schließlich habe ich angeregt, eine interne Übersicht über die in der Handwerkskammer manuell geführten Dateien einzurichten, damit die Datensicherung zuverlässig überwacht werden kann.

Der Prüfungsbericht hat erfreulicherweise dazu geführt, daß alle Handwerkskammern nun gemeinsam die Antrags- und sonstige Datenerhebungsformulare überprüfen.

13.2 Datenerhebung für die Eintragung in die Handwerksrolle

Aufgrund einer Eingabe war die Zulässigkeit von Fragen zu überprüfen, die der Petent vor der Eintragung in die Handwerksrolle der Handwerkskammer zu beantworten hatte. Nach § 17 Abs. 1 der Handwerksordnung ist der Betroffene zu den Angaben verpflichtet, welche die Handwerkskammer benötigt, um gemäß § 16 Abs. 3 zu überwachen, ob ein Handwerk als stehendes Gewerbe entgegen den Vorschriften des Gesetzes ausgeübt wird.

Die Überprüfung ergab, daß die gestellten Fragen im wesentlichen erforderlich sind:

- So muß die Handwerkskammer überprüfen, ob insbesondere bei Gefahrenhandwerken und Gesundheitsberufen durch den angemeldeten Meister der gesamte Betriebsablauf betreut und überwacht wird. Der Meister muß zu diesem Zweck an sämtlichen Werktagen während der ganzen Arbeitszeit **im Betrieb anwesend** sein, um die Mitarbeiter überwachen zu können.
- Die Frage nach einer **früheren Gewerbeuntersagung** ist erforderlich, weil ein technischer Betriebsleiter z.B. bei der BGB-Gesellschaft, OHG oder KG nicht anerkannt werden könnte, wenn gegen ihn bereits eine Gewerbeuntersagung ausgesprochen wurde. Hier soll der Umgehung eines rechtskräftig ausgesprochenen Verbotes der Gewerbebetätigung entgegengewirkt werden.
- Fragen nach Hauptwohnsitz oder Dienstwohnung sind erforderlich, da sie anzeigen, ob der gemeldete Handwerksmeister überhaupt in der Lage ist, seiner Aufsichtspflicht nachzukommen.
- Anstelle der Frage nach **körperlichen, geistigen oder seelischen Gebrechen** genügt allerdings die Vorlage einer ärztlichen Bescheinigung, aus der sich — ohne Nennung einer Diagnose — ergibt, ob gegen die Übernahme der technischen Betriebsleitung ärztlicherseits Bedenken bestehen. Konkretere Fragen wären erst dann zu stellen, wenn Anhaltspunkte für Gebrechen vorliegen, welche den Betriebsleiter als ungeeignet erscheinen lassen.
- Die Frage nach **Verwandtschaft oder Verschwägerung** des Handwerksmeisters mit dem Inhaber hat zwar nicht unmittelbar mit der Eintragung in die Handwerksrolle zu tun. Sie ist aber im Falle einer vereinbarten niedrigen Arbeitsvergütung oder eines im Übergabevertrag vereinbarten niedrigen Übergabeentgelts von Bedeutung. Die Angaben dienen der Klärung der Ernsthaftigkeit der Vereinbarung zugunsten des Antragstellers.
- Auch die Vorlage einer **Krankenkassenbestätigung** über die Anmeldung des Meisters bei der Krankenkasse zeigt die Ernsthaftigkeit der Bestellung zum technischen Betriebsleiter an. Die Vorlage des Arbeitsvertrages allein kann diesen Nachweis nicht ersetzen.
- Die Frage nach der **Lohnsteuerkarte** ist erforderlich als Information darüber, ob die als Betriebsleiter vorgesehene Person weiteren Beschäftigungen nachgeht.
- Nicht als erforderlich erwies sich eine schriftliche Vollmacht, nach der die Sozialversicherungsträger jederzeit Auskünfte an die Handwerkskammer zu erteilen hätten. Eine so weitgehende Vollmacht ist für die Eintragung in die Handwerksrolle nicht erforderlich. Vielmehr genügt es, wenn die Krankenkasse die aktuelle Gehaltshöhe und die Arbeitszeit pro Woche des konkreten Arbeitsverhältnisses mitteilt, damit die Ernsthaftigkeit der Bestellung zum Betriebsleiter überprüft werden kann. Zweckmäßiger ist es freilich, wenn der eintragungswillige Handwerker die Krankenkassenbestätigung selbst vorlegt und nur hilfsweise eine entsprechend beschränkte Vollmacht erteilt.
- Die Vorlage des **Arbeitsvertrages** wurde als Nachweis für die handwerkliche Betriebsleitung für erforderlich angesehen. Soweit der Vertrag nicht schriftlich abgefaßt ist, benötigt die Handwerkskammer eine schriftliche Erklärung beider Seiten, welche die Beurteilung der Ernsthaftigkeit der Vereinbarungen über die Betriebsleitung erlaubt.

Der Fragebogen wird von der Handwerkskammer überarbeitet.

13.3 Datenübermittlung an Berufsvereinigung im Rahmen von Ausnahmebewilligungsverfahren

Eine Eintragung in die Handwerksrolle kann in Ausnahmefällen auch aufgrund einer Ausnahmebewilligung vorgenommen werden. Nach § 8 Abs. 3 Satz 2 der Handwerksordnung hat die Handwerkskammer hierzu die Berufsvereinigung, die der Antragsteller benennt, zu hören.

In der Praxis gibt die Handwerkskammer dem Antragsteller Gelegenheit, gegen die Anhörung einer bestimmten Berufsvereinigung Widerspruch einzulegen. Im Fall eines Widerspruches hat der Bewerber jedoch die Nachteile zu tragen, die sich daraus ergeben, daß deshalb die entscheidungserheblichen Sachverhalte nicht ausreichend aufgeklärt werden können. Daher habe ich angeregt, für den Betroffenen nicht nur die Widerspruchsmöglichkeit vorzusehen, sondern ihm darüber hinaus auch die Benennung einer bestimmten Berufsvereinigung zu ermöglichen. Der Betroffene könnte im Einzelfall deren Anhörung wünschen, weil er seine Interessen dort am ehesten gewahrt sieht. Darüber hinaus sollte er auch die Möglichkeit haben, die Anhörung einer bestimmten Berufsvereinigung ausschließen.

14. Landwirtschaft

14.1 Prüfung eines Amtes für Landwirtschaft

Gegenstand der Prüfung war in erster Linie der Umfang der vom Amt genutzten automatisierten **Dateien** und **Verfahren**. Außerdem wurden **manuelle Karteien** des Amtes einschließlich der erkennbaren regelmäßigen **Datenübermittlungen** überprüft.

Die Überprüfung ergab, daß die den einzelnen Mitarbeitern zugeteilten Zugriffsberechtigungen (Lese- und Änderungsberechtigung) zu automatisierten Dateien teilweise nicht mit dem sachlichen Aufgabenbereich des einzelnen Sachbearbeiters übereinstimmten. Das Amt hat unmittelbar nach dieser Feststellung den Umfang der Zugriffsberechtigungen überprüft und — soweit notwendig — der Zuständigkeit der einzelnen Mitarbeiter angepaßt.

Bei der stichprobenartigen Überprüfung von **Akten** fiel auf, daß dort teilweise aus früherer Zeit **vollständige Steuerbescheide** oder **Pachtverträge** aufbewahrt wurden. Zur Antragsbearbeitung war jedoch nur ein Teil dieser Unterlagen erforderlich. Da die nicht benötigten Daten in Steuerbescheiden und Pachtverträgen im Einzelfall von erheblicher Sensibilität sein können, habe ich empfohlen, auf die Erhebung nicht benötigter Daten zu verzichten. Dies könnte etwa durch Schwärzen der nicht benötigten Teile geschehen. In dem geprüften Amt wurde das Problem jedoch dadurch gelöst, daß inzwischen solche Unterlagen den Antragstellern nach Einsichtnahme in die erforderlichen Angaben ohne Anfertigung von Ablichtungen wieder ausgehändigt werden.

Bei den überprüften **Karteien** haben sich keine Anhaltspunkte für nicht erforderliche Datenerhebung, Speicherung oder Übermittlung ergeben. Zur Vernichtung nicht mehr erforderlicher und nicht zu archivierender Aktenunterlagen habe ich Anregungen gegeben.

15. Statistik

15.1 Volkszählung 1987

Wie in früheren Jahren habe ich die weitere Auswertung der Volkszählungsergebnisse und die Einhaltung des Statistikgeheimnisses kontrolliert. Zur Verbesserung ihrer Planungsunterlagen hat sich eine Reihe von Gemeinden vom Landesamt für Statistik und Datenverarbeitung aus dem Ergebnis der Volkszählung 1987 eine **„Gemeindestatistik nach Blockseiten"** (vgl. 12. Tätigkeitsbericht Nr. 13.2) erstellen lassen. Das Landesamt hat diese Blockseitenstatistiken inzwischen an 68 Gemeinden geliefert. Bei drei kreisfreien Städten, einer Großen Kreisstadt, einer kreisangehörigen Stadt und einer kreisangehörigen Gemeinde habe ich überprüft, ob bei der Übermittlung und Verarbeitung der Blockseitenergebnisse das Statistikgeheimnis und der Datenschutz beachtet werden. Insbesondere war zu prüfen, ob die vom Landesamt gelieferten Blockseitenstatistiken den Vorgaben der §§ 14, 15 Volkszählungsgesetz 1987 entsprechen, eine Identifizierung einzelner Bewohner aufgrund der Angaben in den Blockseitentabellen also ausgeschlossen war.

Entsprechend den Vorgaben der §§ 14 und 15 Volkszählungsgesetz 1987 haben die Statistischen Landesämter bei der Weitergabe von Angaben aus der Volkszählung an Gemeinden zu unterscheiden zwischen Gemeinden **mit** und solchen **ohne** abgeschottete Statistikstellen.

Gemeinden mit abgeschotteter Statistikstelle

Nur Gemeinden mit abgeschotteter Statistikstelle erfüllen die Voraussetzungen des § 14 Abs. 1 Volkszählungsgesetz 1987. Durch das Gesetz zur Ausführung des Volkszählungsgesetzes 1987 (AGVZG 1987) vom 5. März 1987 (GVBl S. 71) und das Bayer. Statistikgesetz ist die Trennung dieser Stellen von anderen kommunalen Verwaltungsstellen sichergestellt. Das Statistikgeheimnis muß durch Organisation und Verfahren gewährleistet sein.

Abgeschottete Statistikstellen sind von den Städten München, Nürnberg, Augsburg, Erlangen, Fürth und Landshut eingerichtet. In drei Städten habe ich geprüft, ob die Statistikstellen **räumlich, sachlich und personell** gegen die allgemeine Verwaltung abgeschottet sind. Mängel konnte ich bei der Überprüfung nicht feststellen.

Gemeinden ohne abgeschottete Statistikstelle

Die Weitergabe von Angaben aus der Volkszählung durch die statistischen Landesämter an Gemeinden ohne abgeschottete Statistikstelle ist einer Veröffentlichung der statistischen Ergebnisse gleichzusetzen und daher nur unter den hierfür gesetzlich festgelegten Voraussetzungen des § 15 Abs. 4 Satz 4 Volkszählungsgesetz 1987 zulässig. Danach müssen bei der Er-

stellung statistischer Ergebnisse in kleinräumiger Gliederung nach Blockseiten, die zur Weitergabe oder Veröffentlichung bestimmt sind, die Gliederungseinheiten Blockseite, soweit sie Einzelangaben enthalten, die dem Auskunftspflichtigen oder Betroffenen zuzuordnen sind, zu höheren Einheiten zusammengefaßt werden.

Bei der Anfertigung und Lieferung der Blockseitenstatistiken an diese Gemeinden haben die statistischen Landesämter und das Statistische Bundesamt zum Schutz des Statistikgeheimnisses folgende Vorkehrungen getroffen: Zum einen werden auf der Basis der Blockseiten nicht Ergebnisse für alle Statistikmerkmale aus der Volkszählung übermittelt, sondern nur ein **erheblich eingeschränkter Merkmalskatalog**. Zum anderen erhalten diese Gemeinden nur **aggregierte**, d.h. zusammengefaßte Daten, die auch mit Zusatzwissen keine Hinweise auf bestimmte Personen zulassen, so daß eine Identifizierung faktisch unmöglich ist („Blockprogramm II").

Inhaltliche Mängel bei den gelieferten Blockseitenstatistiken waren nicht festzustellen. Die Durchsicht der vom Landesamt gelieferten Blockseitentabellen hat ergeben, daß keine Daten enthalten sind, die Hinweise auf bestimmte Personen zulassen. Einzelfälle, d.h. nicht aggregierte Daten, waren in den Blockseitenstatistiken nicht enthalten. Überschreitungen des eingeschränkten Merkmalskatalogs beim Blockprogramm II konnten ebenfalls nicht festgestellt werden.

Auswertung der Blockseitenergebnisse

Ferner habe ich sowohl bei abgeschotteten wie auch bei nichtabgeschotteten Statistikstellen geprüft, ob Mängel bei der Auswertung der Blockseitenergebnisse vorliegen. Hier war darauf zu achten, daß keine Einzelangaben oder Angaben auf kleinräumiger Basis an andere Verwaltungsstellen (insbesondere Planungsreferate) weitergegeben und in Publikationen dieser Städte veröffentlicht werden.

Auch insoweit konnte ich keine Mängel feststellen. Die Volkszählungsergebnisse wurden durchwegs auf „höherer Basis", als dies Block und Blockseite darstellen, weitergegeben oder veröffentlicht, in der Regel auf der Basis von größeren Stadtteilen oder Stadtteilbezirken.

Ich werde auch weiterhin die Einhaltung der Bestimmungen des Volkszählungsgesetzes 1987 überwachen.

15.2 Fragebogen bei der Erstellung der Einzelhandelsstatistik

Ein Apotheker hat mich auf einen Fragebogen aufmerksam gemacht, der vom Statistischen Landesamt bei Erstellung der Einzelhandelsstatistik verwendet wurde. Der Fragebogen besteht aus einem Deckblatt und dem eigentlichen Fragebogen. Das Deckblatt enthielt die vollständige Firmenanschrift. Im Hauptfragebogen mußte der Auskunftspflichtige die Branche und die genaue Anschrift des Unternehmens angeben. Zwar wird das Deckblatt nach der Eingangskontrolle beim Landesamt vernichtet. Da jedoch im Hauptfragebogen der Auskunftspflichtige die Branche und die genaue Anschrift des Unternehmens anzugeben hatte, war der Apotheker der Auffassung, es bedürfe nicht viel Sachverstands, um die Daten zusammenzuführen und damit die Anonymisierung der Einzelhandelsstatistik zunichte zu machen.

Aus der Stellungnahme des Landesamts ergab sich, daß die verwendeten Fragebögen längere Zeit nicht mehr überarbeitet worden und deshalb datenschutzrechtlich nicht mehr auf dem neuesten Stand waren. Das Landesamt hat die Fragebögen zwischenzeitlich geändert; die Angabe der Anschrift im Fragebogen wird von den Auskunftspflichtigen nicht mehr verlangt.

15.3 Faktische Anonymisierung bei Übermittlung von Einzelangaben von Statistikämtern an Hochschulen

Für die Durchführung wissenschaftlicher Vorhaben dürfen gem. § 16 Abs. 6 Bundesstatistikgesetz von den statistischen Ämtern Einzelangaben an Hochschulen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermittelt werden, wenn diese Einzelangaben nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können und die Empfänger besonders zur Einhaltung des Statistikgeheimnisses verpflichtet worden sind (faktische Anonymisierung). Diese Bestimmungen gelten auch für Einzelangaben aus der Volkszählung 1987.

Über die Frage, welche Anforderungen an die faktische Anonymisierung zu stellen sind, herrschte bisher Unklarheit. Während die Wissenschaftler an möglichst genauen Informationen interessiert sind, muß von seiten des Datenschutzes darauf geachtet werden, daß eine Identifizierung einzelner Personen ausgeschlossen ist.

Zur Lösung dieses Problems wurde 1987 die Universität Mannheim (Lehrstuhl für Methoden der empirischen Sozialforschung und angewandte Soziologie) mit der Erarbeitung eines wissenschaftlichen Projekts beauftragt. Dieses „Anonymisierungsprojekt" wurde 1991 im Arbeitskreis Statistik der Datenschutzbeauftragten des Bundes und der Länder erörtert.

Das Gutachten der Universität Mannheim hat den praktischen Fall untersucht, ob durch einen Vergleich der Mikrozensusdaten aus dem Jahr 1987 mit dem Gelehrtenhandbuch aus dem Jahre 1985 einzelne Personen (im wesentlichen Hochschullehrer) identifiziert werden können. Das Gutachten kommt zum Ergebnis, daß eine Identifizierung von Hochschulleh-

rern bei Anwendung der im einzelnen beschriebenen Methoden und Vorkehrungen so gut wie nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Solche Methoden und Vorkehrungen sind z.B.:

- technisch-organisatorische Schutzmaßnahmen zur Kontrolle der Datennutzung
- ausdrückliche vertragliche Bindung des Datenempfängers (Hochschule), daß er sich an die technisch-organisatorischen Schutzmaßnahmen hält, einschließlich Vereinbarung einer Vertragsstrafe
- Geheimhaltung der lokalen Umsetzung von Stichprobenplänen
- systemfreie Anordnung der Daten (im Gegensatz zur systematischen Anordnung z.B. nach räumlichen Kriterien)
- falls erforderlich Merkmalvergröberungen u.a.

Bei Beachtung der im Gutachten dargestellten Schutzmaßnahmen bestehen keine datenschutzrechtlichen Bedenken gegen die Anonymisierungsmethode.

15.4 Weitergabe der Viehzählungslisten durch Gemeinden an Veterinärämter für tierseuchenrechtliche Maßnahmen

Eine Gemeinde hat angefragt, ob sie die Viehzählungslisten dem Staatlichen Veterinäramt zur Erfüllung der tierseuchenrechtlichen Vorschriften überlassen dürfe.

In Übereinstimmung mit dem Innenministerium habe ich diese Frage verneint. Für die Viehzählungsstatistik gilt ebenso wie für andere Statistiken das Geheimhaltungsgebot sowie das Gebot der Trennung zwischen Statistik und Verwaltungsvollzug gem. § 16 Abs. 1 Bundesstatistikgesetz. Danach dürfen die Viehzählungsunterlagen (einzelne Erhebungsbögen oder Listen) nur für die Erstellung der Viehzählungsstatistik durch das Statistische Landesamt benutzt werden. Ihre Verwendung für andere Verwaltungszwecke, z.B. für tierseuchenrechtliche Maßnahmen, ist unzulässig, soweit der Betroffene nicht ausdrücklich eingewilligt hat wie etwa zur Berechnung der Tierseuchenbeiträge. Aber auch im letzteren Fall dürfen die Unterlagen nicht für weitere Zwecke verwendet werden.

15.5 Viehzählung — Statistikgeheimnis, Aufbewahrung von Viehzählungsunterlagen

Ein Landwirt beschwerte sich darüber, daß der 1. Bürgermeister in öffentlicher Gemeinderatssitzung, bei der über einen Bebauungsplan beraten wurde, Einzelheiten aus den Viehzählungsunterlagen der letzten fünf Jahre bekanntgegeben habe.

Meine Ermittlungen ergaben, daß der Bürgermeister durch die Verwendung von Angaben aus der Viehzählung im Bebauungsplanverfahren gegen den Zweckbindungsgrundsatz verstoßen hat. Die Gemeinde wurde beanstandet.

In diesem Zusammenhang ging ich der Frage nach, weshalb bei den Gemeinden Viehzählungsunterlagen über mehrere Jahre hinweg aufbewahrt werden und ob dabei gegen das Statistikgeheimnis verstoßen wird. Meinen Feststellungen zufolge werden die Erhebungsbögen (3fach) wie folgt behandelt:

1. Das Original des Viehzählungsbogens geht an das Landesamt für Statistik und Datenverarbeitung, das hieraus die Viehzählungsstatistik erstellt.
2. Ein Durchschlag verbleibt beim Landwirt.
3. Der zweite Durchschlag dient der Gemeinde zur Erstellung der Tierseuchenbeitragsliste für die Bayer. Versicherungskammer (Tierseuchenkasse), sofern sich der Tierhalter mit dieser Nutzung seiner Viehzählungsdaten ausdrücklich einverstanden erklärt hat.

Mit der Einwilligung des Landwirts in die Nutzungsänderung (hier: Tierseuchenbeitragsberechnung) verlieren die Viehzählungserhebungsbögen (Durchschläge) ihre Eigenschaft als Statistikdaten und unterliegen nicht mehr dem restriktiven Statistikgeheimnis. Allerdings dürfen die Viehzählungsdaten außer zur Berechnung der Tierseuchenbeiträge für keinen anderen Zweck verwendet werden (z.B. für die Berechnung der Wasserversorgungsbeiträge), soweit der Betroffene nicht ausdrücklich eingewilligt hat.

Wie bei anderen öffentlichen Beiträgen müssen die Unterlagen gewisse Zeit aufbewahrt werden. Die Aufbewahrungsdauer muß mit dem Innenministerium noch geklärt werden.

16. Schulwesen

16.1 Verwendung von Echtdaten in der Landwirtschaftsschule

Ein Vater wandte sich mit folgendem Anliegen an mich:

Sein Sohn beabsichtige, nach Abschluß der Berufsschule die weiterführende Landwirtschaftsschule zu besuchen. Als eine Zulassungsvoraussetzung für den Übertritt habe die Schule Echtdaten über die Einkommens- und Eigentumsverhältnisse des elterlichen Betriebes einschließlich der dazugehörigen Unterlagen (Urkunden, Kontoauszüge, Angaben zum Viehbestand, Verzeichnis der Maschinen usw.) zu einem bestimmten Stichtag angefordert.

Eine Nachfrage bei der Berufsschule ergab, daß nicht die Schule, sondern der Ausbildungsberater des Landwirtschaftsamtes diese Angaben verlangt hatte. Ein Zusammenhang zwischen dem Übertritt an die Landwirtschaftsschule und den angeforderten Daten

bestehe nicht. Die Daten würden vielmehr für folgende Zwecke verwendet: Um die Studierenden der Landwirtschaftsschule auf ihren späteren Beruf als Betriebsleiter vorzubereiten, müßten sie am Ende der Ausbildung u.a. die Fertigkeit besitzen, die Eröffnungsbilanz für den eigenen Betrieb zu erstellen und die laufenden Buchungen fehlerfrei durchzuführen. Deshalb hätten die Studierenden die Möglichkeit, **mit Einverständnis der Eltern** den eigenen Betrieb zu bebuchen. Hierzu müßten zu Beginn des Studiums die für die Eröffnungsbilanz nötigen Betriebsdaten zum Bilanzstichtag erhoben und anschließend Aufzeichnungen über Einnahmen und Ausgaben geführt werden. Für den Fall, daß Echtdaten verwendet würden, sehe der Lehrplan vor, die Daten ausschließlich auf einer Diskette zu speichern, die Eigentum des Studierenden bleibe. Die Verwendung von Echtdaten habe gegenüber den bisher verwendeten fiktiven Zahlen den Vorteil der Praxisnähe. Soweit Eltern hiergegen aber Bedenken erheben, könnten weiterhin fiktive Daten eines Beispielbetriebes verwendet werden.

Gegen diese Praxis bestehen nur dann keine Bedenken, wenn die Landwirtschaftsschule deutlich darauf hinweist, daß Echtdaten **freiwillig** verwendet werden **können**. Erforderlich ist die Aufklärung über die Art der Verwendung und über die etwaige Gefährdung der Vertraulichkeit der Echtdaten sowie die **ausdrückliche** Zustimmung der Eltern. Ferner dürfen die Echtdaten ausschließlich für Ausbildungszwecke verwendet werden.

16.2 Hinweis auf die Aufnahmeprüfung im Notenbogen der Abschlußklasse

Erfüllen Schüler nicht die regulären Voraussetzungen für die Aufnahme in die Realschule, so haben sie die Möglichkeit, durch Teilnahme am Probeunterricht ihre Befähigung nachzuweisen. Auch die Aufnahme in eine höhere Jahrgangsstufe setzt das Bestehen einer Aufnahmeprüfung und einer Probezeit voraus.

Schüler einer 10. Klasse Realschule haben mir in diesem Zusammenhang folgende Frage gestellt: „Ist ein Zusatz im Notenbogen der 10. Klasse, daß ein Schüler mit Aufnahmeprüfung in die 7. Klasse der Realschule gekommen ist, für die zehnten Klassen noch erforderlich?". Nach Auffassung der Schüler besteht die Gefahr, daß dadurch ein Lehrer bei der Vergabe der Zeugnis- bzw. Prüfungsnoten in seinem objektiven Urteil beeinflußt wird.

Mit dem Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst bin ich der Auffassung, daß der Hinweis auf die um Jahre zurückliegende Aufnahmeprüfung im Notenbogen der Abschlußklasse nicht mehr zulässig ist. Bei dem Notenbogen handelt es sich um einen Universalschülerbogen, der für alle Jahrgangsstufen verwendet werden kann. Da für jeden Schüler pro Schuljahr ein neuer Notenbogen angelegt wird, ist ein Hinweis auf eine eventuelle Teilnahme am Probeunterricht nur für die 7. Jahrgangsstufe und ein Hinweis auf eine Aufnahmeprüfung nur bei Eintritt in eine höhere Jahrgangsstufe von Bedeutung. In diesen Fällen darf ein Eintrag in den Notenbogen dieser Jahrgangsstufe erfolgen, da er den Lehrern Hinweise auf eine laufende Probezeit oder ihre Verlängerung gibt.

Da diese Vermerke für die 10. Jahrgangsstufe jedoch nicht mehr von Bedeutung sind, wäre ein entsprechender Eintrag im Notenbogen der 10. Klasse datenschutzrechtlich unzulässig. Dies dürfte für vorausgehende Jahrgangsstufen entsprechend gelten.

16.3 Offenbarung von Sozialhilfedaten an Fachoberschüler

Eine Stadt fragte an, inwieweit im Blick auf das Sozialgeheimnis Fachoberschülern der Fachrichtung Soziales, die beim Sozialamt ihre fachpraktische Ausbildung ableisten, Zugang zu Akten und Dateien gewährt werden darf.

In Abstimmung mit den zuständigen Ministerien habe ich folgende Auffassung vertreten:

Während der Ableistung der fachpraktischen Ausbildung unterliegen die Praktikanten als Schüler weiterhin in vollem Umfang der Schulordnung für Fachoberschulen. Nach § 14 Abs. 4 Satz 3 besteht Verschwiegenheitspflicht für alle Angelegenheiten, die den Schülern im Rahmen der fachpraktischen Ausbildung in außerschulischen Einrichtungen zur Kenntnis gelangen, soweit diese der Geheimhaltung unterliegen. Hierzu zählt auch der Inhalt von Akten, Dateien oder anderen Unterlagen, welche die Schüler zur Anfertigung von Aufgaben oder zur Bearbeitung von Einzelfällen im Rahmen ihrer Ausbildung benötigen. Nach § 14 Abs. 4 Satz 1 haben sie außerdem den Anordnungen der Ausbilder Folge zu leisten.

Die „Richtlinien für die fachpraktische Ausbildung von Fachoberschülern" sehen zu Beginn der fachpraktischen Ausbildung eine Belehrung über die Verschwiegenheitspflichten nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) vor, die durch Unterschrift zu bestätigen ist. Zudem erhalten die Schüler eine Zusammenstellung der einschlägigen strafrechtlichen Bestimmungen sowie einen Abdruck des Verpflichtungsgesetzes und der unterzeichneten Niederschrift über die Verpflichtung.

Ich bin allerdings der Auffassung, daß eine generelle unkontrollierte Einsichtsmöglichkeit in **alle** vorhandenen Unterlagen, beispielsweise ein systematisches Durchsuchen der Registratur oder Karteien nach bestimmten Namen zu weit geht und zur Aufgabenerfüllung auch nicht erforderlich ist. Insoweit hat der Ausbildungsleiter die fachpraktische Ausbildung zeitlich und organisatorisch sinnvoll zu gestalten und die Einsichtnahme in Vorgänge, die dem Sozialge-

heimnis unterliegen, auf das für die Ausbildung Notwendige zu beschränken.

16.4 Meldung von Schulunfällen an den Bayerischen Gemeindeunfallversicherungsverband

Eine Schule fragte an, ob sie dem Gemeindeunfallversicherungsverband bei einem Schulunfall die Daten der Krankenkasse des Schülers bzw. die Daten der Krankenkasse seiner Eltern mitteilen dürfe.

Der Gemeindeunfallversicherungsverband ist als ein Träger der gesetzlichen Unfallversicherung befugt, die für die Abwicklung der Unfallversicherung einschließlich etwaiger Schadensersatzansprüche erforderlichen Daten bei der Behörde zu erheben, in deren Zuständigkeitsbereich sich der Unfall ereignet hat. Diese hat ihm den Unfall nach § 1553 Abs. 1 Reichsversicherungsordnung (RVO) anzuzeigen.

Nach Art. 62 Abs. 1 Satz 1 Bayerisches Erziehungs- und Unterrichtsgesetz (BayEUG) ist die Erhebung und Verarbeitung von Daten zur Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben zulässig. § 1552 RVO weist dem Leiter der Dienststelle oder seinen Beauftragten die Aufgabe zu, binnen drei Tagen, nachdem er vom Unfall erfahren hat, eine Unfallanzeige zu erstatten. Soweit der Schule die benötigten Daten des Schülers nicht bereits im Schülerbogen oder im Schulverwaltungsprogramm vorliegen, ist die Schule zur Erhebung der übrigen Daten berechtigt. Hierunter fällt neben Angaben zum Unfallhergang (verletzte Körperteile, Art der Verletzungen) auch die Frage nach der zuständigen Krankenkasse, mit der sich der Träger der Unfallversicherung zur Abwicklung der Schadensansprüche direkt in Verbindung setzen kann.

17. Hochschule

Prüfung von Hochschulen

Im Berichtszeitraum habe ich eine Universität und eine Fachhochschule, und zwar die **Studentenverwaltung** und einzelne **Lehrstühle** bzw. **Fachbereiche** geprüft. Zusammenfassend ist festzustellen, daß der Datenschutz insgesamt beachtet wird. Allerdings zwingen hohe Studentenzahlen oft zu Verfahren, die eine möglichst reibungslose, einfache und rasche Abwicklung der Verwaltungsaufgaben gewährleisten. Dabei kommt es dann vor, daß nicht alle Anforderungen des Datenschutzes eingehalten werden können.

So war festzustellen, daß **Personalbögen** von Studenten, die gleichzeitig Zeugnisse, Lebenslauf und weitere Nachweise enthalten, im Immatrikulationsamt in offenen raumhohen Regalen ohne jegliche Verschlußmöglichkeit aufbewahrt werden. Zugang zu dem Raum haben zwar auch die Studenten, die sich immatrikulieren. Während der Öffnungszeiten ist das Zimmer jedoch mit Personal der Universitätsverwaltung besetzt. Bei Verlassen des Raums wird dieser abgesperrt. Allerdings nimmt ein **Reinigungsdienst** in der Regel nach Dienstschluß Reinigungsarbeiten vor. Ich habe gefordert, das Immatrikulationsamt nur unter Aufsicht reinigen zu lassen.

Auch **Krankenversicherungsbescheinigungen**, die laufend neu einsortiert werden müssen, finden sich in offenen Karteikästen im Zimmer des Sachbearbeiters, weil sich die dafür vorgesehene Aufbewahrung in abschließbaren Stahlschränken als sehr unpraktisch erwiesen hat. Ich habe auch hier angeregt, eine Lösung zu suchen, die auch den Belangen des Datenschutzes Rechnung trägt.

An einem Lehrstuhl habe ich die Erstellung einer **Dienstanweisung** für die Vernichtung von personenbezogenen Unterlagen angeregt. Sie wurde mittlerweile erlassen.

Derzeit wird noch geprüft, ob die **Notenbögen** von Studenten, die kurs- bzw. seminarweise abgelegt und in verschlossenen Stahlschränken aufbewahrt werden, unbegrenzt vorgehalten werden müssen oder ob eine Aussonderungsfrist gefordert werden soll.

18. Archiv und Forschung

18.1 Prüfung des Landesamts für Denkmalpflege

Bei der Prüfung des Bayer. Landesamts für Denkmalpflege waren gravierende Mängel nicht feststellbar. Im einzelnen habe ich folgendes gefordert:

- Die Datei „Archäologisch-Topographisches Planarchiv", in der obertägige Bodendenkmäler kartographisch zum Zwecke der Inventarisation und der Erforschung der Denkmäler dokumentiert sind, enthält als personenbezogene Daten die Nummer der Gemarkung, in der das Bodendenkmal liegt, sowie den Namen des Eigentümers, auf dessen Grund das Bodenmerkmal gefunden wurde. Da die Datei, die auch eine große Anzahl nicht personenbezogener Daten speichert, noch nicht freigegeben und zum **Datenschutzregister** gemeldet wurde, habe ich gefordert, dies nachzuholen.
- In der Personalkartei habe ich auf den Personalkarten neben der **„Konfession"** auch Angaben zu **Name und Geburtsdatum der Kinder** vorgefunden. Da die Besoldung, für die diese Daten erforderlich sind, nicht vom Personalreferat, sondern von einer anderen Behörde miterledigt wird, habe ich um Überprüfung und entsprechende Reduzierung der Speicherungen gebeten.
- Schließlich sind noch Fragen der datenschutzgerechten Aufbewahrung verschiedener Karteien zu klären.

Bei der Prüfung habe ich auch festgestellt, daß das Landesamt auf Anfrage Abgeordneten, Landräten und anderen Politikern über die Gewährung von Zuschüssen nach Art. 22 Denkmalschutzgesetz sowie aus dem Denkmalschutzfonds, auch über die Höhe der Zuschüsse, **Auskunft** erteilt. Ich halte solche Auskünfte nur mit Zustimmung des Zuschußempfängers für zulässig. Zu dieser Frage habe ich das Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst um Stellungnahme gebeten (vgl. auch Nr. 18.2).

18.2 Veröffentlichung von Zuschüssen aus Mitteln des Entschädigungsfonds nach dem Denkmalschutzgesetz

Ein Verband, zu dessen Mitgliedern auch Eigentümer von denkmalgeschützten Bauwerken gehören, schilderte mir folgendes Problem:

Aus dem Entschädigungsfonds, den die Oberste Denkmalschutzbehörde nach Art. 21 Denkmalschutzgesetz eingerichtet hat, können für die Instandsetzungs- und Schutzmaßnahmen an Baudenkmälern Zuschüsse gewährt werden, wenn und soweit dem Eigentümer die meist sehr hohen Kosten nicht zugemutet werden können.

Die **Höhe** der gewährten Zuschüsse sowie **das geförderte Objekt** werden von der Obersten Denkmalschutzbehörde **veröffentlicht**. Dies wird mit dem Interesse der Öffentlichkeit am Denkmalschutz begründet. Gleichzeitig sollen privates Engagement gefördert und die Vergabe der Zuschüsse transparent gemacht werden.

Gegen die Veröffentlichung der genauen Höhe der Zuschüsse und der geförderten Objekte wehren sich die Eigentümer von Baudenkmälern: Zwar enthalte die Veröffentlichung nicht den **Namen** des Begünstigten, jedoch sei dieser durch Nennung des geförderten Objekts leicht in Erfahrung zu bringen. Damit werde in der Bevölkerung die genaue Höhe des Zuschusses bekannt den ein Denkmalbesitzer erhalten habe. Unmut und Neidäußerungen seien die Folge, da sich die wenigsten Leute Vorstellungen über die laufenden Belastungen des Eigentümers machen könnten. Im Ergebnis führe dies zu einem unguten Verhältnis zwischen Denkmalbesitzern und sonstiger Bevölkerung. Im einen oder anderen Fall habe dies bereits so abschreckend gewirkt, daß notwendige Erhaltungsmaßnahmen hinausgeschoben würden oder ganz unterblieben seien.

Aus datenschutzrechtlicher Sicht ist anzumerken: Nach Art. 18 Abs. 1 Bayerisches Datenschutzgesetz ist eine Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs — um eine solche handelt es sich bei der Veröffentlichung — nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der übermittelnden Stelle zugewiesenen Aufgaben erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Zu den schutzwürdigen Belangen zählt hier das allgemeine Persönlichkeitsrecht und hieraus abgeleitet das Recht auf **Wahrung der Privatsphäre**, das durch gewisse „Anfeindungen" von seiten Dritter gestört werden kann. Dem stehen die berechtigten Interessen der Öffentlichkeit an der Veröffentlichung der Daten zur Transparenz des Verwaltungshandelns bei der Vergabe von Zuschüssen gegenüber. Allerdings dürften hier die schutzwürdigen Interessen der Zuschußempfänger überwiegen.

Ich habe deshalb vor kurzem dem Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst vorgeschlagen, die Höhe des Zuschusses und das geförderte Objekt nur noch dann zu veröffentlichen, wenn der Zuschußempfänger vorher zugestimmt hat. Die Stellungnahme der Obersten Denkmalschutzbehörde bleibt abzuwarten.

18.3 Datenschutz bei Dissertationen

Einsicht in Personenstandsregister

Eine Doktorandin fragte, ob es zulässig sei, im Rahmen ihrer Dissertation über „die Bevölkerung jüdischer Landgemeinden in Bayern 1861—1933" Einsicht in die Personenstandsregister der Standesämter zu nehmen.

Das Personenstandsgesetz gewährt bisher eine solche Auswertung der Personenstandsunterlagen nur bei Vorliegen eines **rechtlichen** Interesses. Die Einsichtnahme ist demnach nur zulässig, wenn sie zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen unerläßlich ist. Nicht hierunter fällt die allgemeine Einsichtnahme in Personenstandsunterlagen im Rahmen der Durchführung eines Forschungsvorhabens. Daran ändert auch die in Art. 5 Abs. 3 Grundgesetz gewährleistete Forschungsfreiheit nichts. Für das Standesamt geht der Persönlichkeitsschutz der in den Personenstandsbüchern eingetragenen Personen nach geltendem Recht vor.

Jedoch ist inzwischen auch anerkannt, daß der Zugang zu Personenstandsbüchern zum Zwecke der wissenschaftlichen Forschung überdacht werden muß. Der Bundesgesetzgeber beabsichtigt deshalb, das Personenstandsgesetz zugunsten der wissenschaftlichen Forschung zu ändern.

Bis zu einer Gesetzesänderung ist es jedoch den Standesbeamten verwehrt, eine Einsichtnahme in die Personenstandsbücher zum Zwecke der Dissertation zu ermöglichen.

Anonymisierung und Schutzfristen

Eine andere Doktorandin fragte, ob der Persönlichkeitsschutz verletzt werde, wenn sie in ihrer Doktorarbeit über eine bayerische Judengemeinde im Zeitraum von 1684 — 1942 frühere Personen, die sich im

NS-Staat aktiv betätigten und insbesondere an Ausschreitungen gegen Juden, „Arisierungen" o.ä. beteiligt waren, mit Namen oder mit den jeweiligen Anfangsbuchstaben kennzeichne. Zudem wies sie darauf hin, innerhalb der Bevölkerung würde nur noch ein Teil der älteren Generation die Namen der Personen kennen, die im Dritten Reich in irgendeiner Weise hervorgetreten seien. Die Doktorandin hatte für ihre Dissertation Spruchkammerakten eingesehen.

Unabhängig davon, ob die eingesehenen Spruchkammerakten bereits archiviert waren oder nicht, macht der oben geschilderte Fall wieder einmal das Spannungsverhältnis zwischen Persönlichkeitsschutz auf der einen und Wissenschaftsfreiheit auf der anderen Seite deutlich. Es ist leicht nachvollziehbar, daß eine wissenschaftliche Arbeit zur Zeitgeschichte nicht ganz ohne das Auftreten von Personen auskommen kann. Diese wiederum berufen sich auf ihr Persönlichkeitsrecht und — daraus abgeleitet — die Wahrung ihrer Privatsphäre.

Das am 1.1.1990 in Kraft getretene Archivgesetz hat zum Schutz der Persönlichkeitsrechte Schutzfristen vorgesehen sowie eine Einsichtnahme in archivierte Unterlagen von Auflagen abhängig gemacht, nämlich dann, wenn Grund zu der Annahme besteht, daß schutzwürdige Belange Betroffener oder Dritter entgegenstehen.

In der Praxis sieht dies so aus, daß Wissenschaftler, die Einsicht in archivierte Akten erhalten, eine Auflage mit der Maßgabe unterschreiben, Personen so zu anonymisieren, daß sie nicht wiedererkennbar sind. Hierzu reichen nicht in jedem Fall die Abkürzung der Namen auf ihren Anfangsbuchstaben aus. Gegebenenfalls müssen auch fiktive Initialen verwendet werden. Namen dürfen nur dann genannt werden, wenn sie für die wissenschaftliche Aussagekraft einer Forschungsarbeit „unerläßlich" sind. Dies ist in jedem Einzelfall festzustellen, wobei letztlich der veröffentlichende Wissenschaftler die Abwägung vorzunehmen hat, ob ein Name veröffentlicht werden soll oder nicht. Dafür trägt er auch die rechtlichen Konsequenzen.

Eine Ausnahme vom Grundsatz der Anonymisierung erfahren „Personen der Zeitgeschichte", bei denen nicht nur an überregional bekannte Politiker oder Personen des öffentlichen Lebens zu denken ist. Hierunter fallen auch Personen, die auf örtlicher Ebene allgemein bekannt sind oder waren. Dies gilt beispielsweise für die Namen der damaligen Ortsgruppenleiter oder Bürgermeister.

Obwohl durch die Festlegung von Schutzfristen Archivgut, das sich auf natürliche Personen bezieht (personenbezogenes Archivgut) erst 10 Jahre nach dem Tod des Betroffenen bzw. 90 Jahre nach dessen Geburt benützt werden darf (Art. 10 Abs. 3 ArchivG), wirken nach allgemeiner Meinung die Persönlichkeitsrechte auch darüber hinaus noch bis zu 30 Jahre nach dem Tod nach.

18.4 Standesamtswesen — genealogische Forschung

Wieder haben sich Familienforscher beklagt, weil § 61 Abs. 1 Personenstandsgesetz keine Auskünfte über längst verstorbene Vorfahren (insbesondere der Seitenlinie) sowie über längst verstorbene Personen, die keine lebenden Abkömmlinge mehr haben, zuläßt.

Die Benutzung der Personenstandsbücher (Einsicht und Durchsicht dieser Bücher sowie Erteilung von Personenstandsurkunden) wird abschließend in § 61 Personenstandsgesetz (PStG) geregelt. § 61 Abs. 1 PStG unterscheidet bei den Benutzungsberechtigten zwischen uneingeschränkt berechtigten Personen, Behörden und sonstigen Personen. Uneingeschränkt Berechtigte sind Personen, auf die sich der Eintrag bezieht, sowie ihre Vorfahren, Abkömmlinge und Ehegatten. Behörden sind nur im Rahmen ihrer Zuständigkeit benutzungsberechtigt. Sie haben zum Nachweis ihrer Berechtigung dem Standesbeamten den Zweck anzugeben, für den sie die Personenstandsbücher benutzen möchten. Andere Personen sind nur dann berechtigt, wenn sie ein **rechtliches Interesse** glaubhaft machen. Dies wäre beispielsweise der Fall, wenn die Einsichtnahme der Verfolgung von Rechten oder der Abwehr von Ansprüchen dienen würde.

Obwohl ich für das Anliegen der Familienforscher Verständnis habe, sehe ich bei der bestehenden Rechtslage, insbesondere wegen des fehlenden **rechtlichen Interesses**, keine Möglichkeit, dem Einsichtbegehren der Genealogen zu entsprechen.

Ergänzend ist noch anzumerken, daß sogar öffentlichen Hochschulen und ihren Instituten die Benutzung der Personenstandsbücher für Forschungszwekke nach Art. 61 PStG verwehrt ist. Dies hat beispielsweise das Landgericht Frankenthal in seinem Beschluß vom 30.01.1985 unter Hinweis auf das Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) bestätigt.

19. Umweltfragen

Umfrage eines Landkreises zum Abfallverhalten

Am 1. März 1991 ist das Bayerische Abfallwirtschafts- und Altlastengesetz in Kraft getreten. Es sieht als vorrangige Ziele der Abfallwirtschaft die Abfallvermeidung, Schadstoffminimierung sowie die stoffliche Abfallverwertung vor. Angefallene Abfälle, insbesondere Glas, Papier, Metall, Kunststoff, Bauschutt und kompostierbare Stoffe sollen weitgehend in den Stoffkreislauf zurückgeführt werden.

Um das Gesetz zu vollziehen, noch bestehende Informationsdefizite der Bürger kennenzulernen, aber auch um Anregungen für ein Müllkonzept zu erhalten, veranstaltete ein Landkreis eine große Umfrage auf freiwilliger Basis.

Zur Vorprüfung legte er mir einen Fragebogen für eine Bürgerbefragung zur Abfallwirtschaft vor, der u.a. folgende Fragen enthielt: Halten Sie das Containernetz im Landkreis für ausreichend? Sind Sie mit dem Recyclinghof in Ihrer Gemeinde zufrieden? Kompostieren Sie selbst? Was machen Sie mit dem in Ihrem Haushalt anfallenden Biomüll und den organischen Gartenabfällen? Wie stehen Sie zur Einführung der Biotonne?

Neben den Fragen zum Abfallverhalten waren auch folgende Angaben zur Person vorgesehen: Alter, Geschlecht, Beruf, Familienstand, Wohnort, Gemeinde, Haushaltsgröße sowie Doppel-, Reihen- oder Mehrfamilienhaus.

Neben der Bitte, möglichst zahlreich an der Fragebogenaktion teilzunehmen, versicherte die Abteilung Öffentlichkeitsarbeit außerdem, daß „die Anonymität selbstverständlich gewahrt bleibe".

Daran hatte ich allerdings meine Zweifel. Aufgrund der bestehenden Konzeption der personenbezogenen Angaben erscheint es im Einzelfall nicht ausgeschlossen, einzelne Personen aufgrund der genauen Angaben zu Beruf, Alter, Familienstand, Haushaltsgröße und Gemeindenamen zu identifizieren. Damit könnten aber genaue Aufschlüsse über deren bisheriges oder beabsichtigtes Abfallverhalten gewonnen werden. Auch um zu vermeiden, daß Bürger aus Angst vor einer solchen Identifizierung an der Bürgerbefragung nicht teilnehmen und damit den Aussagewert der Ergebnisse mindern, habe ich empfohlen, die Fragen zu den persönlichen Angaben so zu gestalten, daß die Anonymität besser sichergestellt ist. Dies wird beispielsweise dadurch erreicht, daß

- die Frage nach dem genauen Alter durch Feldvorgaben für Altersgruppen ersetzt wird,
- an Stelle der genauen Berufsangabe eine Zuordnung zu einer Berufsgruppe (z.B. selbständig, Arbeiter, Rentner) möglich ist,
- an Stelle des Familienstandes nach Ein- oder Mehr-Personenhaushalt gefragt wird.

20. Verkehrswesen

20.1 Speicherung von Unschuldigen in „Schwarzfahrerdateien"

Im 12. Tätigkeitsbericht habe ich auf den in der Presse ausführlich berichteten Vorfall hingewiesen, daß ein Unschuldiger, dessen Name ein unbekannter Schwarzfahrer bei einer Fahrscheinkontrolle angegeben hatte, in der Schwarzfahrerkartei der Deutschen Bundesbahn gespeichert war. Diesen Fall hatte ich zum Anlaß genommen, mich bei den Stadtwerken München nach deren Praxis zu erkundigen. Die Stadtwerke München hatten mitgeteilt, daß auch sie Unschuldige speichern, allerdings mit dem Zusatz, daß ein Fall von „Namensmißbrauch" vorliege und daß die Speicherung auf ausdrücklichen Wunsch gelöscht werde. Solange die Löschung nicht ausdrücklich gewünscht werde, bleibe die Person gespeichert um im Wiederholungsfall den Täter leichter überführen zu können. Diese Speicherung habe ich nicht akzeptiert. Ich hatte gegenüber den Stadtwerken München darauf hingewiesen, daß eine Speicherung Unschuldiger, auch mit dem Zusatz „Namensmißbrauch" datenschutzrechtlich ein gravierender Eingriff und deshalb nicht zulässig ist.

Die Stadtwerke München haben mir daraufhin im Berichtszeitraum mitgeteilt, sie wollten, um meinen datenschutzrechtlichen Bedenken Rechnung zu tragen, die Unbeteiligten, deren Namen mißbraucht worden sind, nur mehr **mit deren Einverständnis** speichern. Sie würden diese Personen anschreiben, über den Sinn der Speicherung informieren und dem Schreiben eine „Widerspruchserklärung" beilegen. Sofern der Betroffene nicht widerspreche, gingen die Stadtwerke davon aus, daß er mit der Speicherung einverstanden sei.

Dieser Vorschlag ist zwar eine wesentliche Verbesserung gegenüber dem bisher praktizierten Verfahren, stellt jedoch noch keine befriedigende Lösung dar. Ich habe deshalb den Stadtwerken nahegelegt, eine **echte „Einverständnislösung"** zu suchen. Dies würde bedeuten, daß die Stadtwerke die Personen, deren Namen mißbraucht worden sind, um ihr **ausdrückliches Einverständnis** zu der Speicherung bitten. Wenn sich ein Betroffener nicht äußert, darf er auch nicht gespeichert werden.

Eine Antwort der Stadtwerke steht noch aus.

20.2 Auskünfte der Kraftfahrzeugzulassungsstellen an Rundfunkanstalten

Im 12. Tätigkeitsbericht habe ich auf Seite 53 festgestellt, daß die Kfz-Zulassungsstellen den Beauftragten der Rundfunkanstalten die Halter von Kraftfahrzeugen nicht mitteilen dürfen zur Prüfung der Frage, ob eine **Rundfunkgebührenpflicht** des Halters besteht.

Das Straßenverkehrsgesetz enthält keine Rechtsgrundlage für solche Auskünfte. Auskünfte erhalten die **Kreisverwaltungsbehörden**, die für die **Verfolgung einer Ordnungswidrigkeit** gem. Art. 9 Abs. 1 Nr. 1 Rundfunkgebührenstaatsvertrag (Bereithalten eines Rundfunkgerätes ohne Anmeldung) **zuständig** sind. Um dennoch an die Halterdaten zur Prüfung der Gebührenpflicht zu gelangen, hat der Bayer. Rundfunk

zunächst folgendes Verfahren — das ihn freilich auch nicht befriedigt hat — zur Diskussion gestellt:

Der Rundfunk stellt gegenüber der Kreisverwaltungsbehörde einen Antrag auf Verfolgung der Ordnungswidrigkeit hinsichtlich des unbekannten Halters eines Kraftfahrzeugs, ohne zu wissen, ob das Rundfunkgerät der Gebührenpflicht unterliegt und ob es angemeldet ist. Dabei würde gegenüber der Kreisverwaltungsbehörde ein Antrag auf Verfolgung einer Ordnungswidrigkeit gestellt, obwohl zum Zeitpunkt der Anzeigeerstattung **keine Anhaltspunkte** für eine Ordnungswidrigkeit vorliegen. Der Rundfunk würde also **ohne Anfangsverdacht** die Anzeige erstatten.

Gegenüber dem Bayer. Rundfunk habe ich darauf hingewiesen, daß ich dieses Verfahren nicht für zulässig halte. Die Einleitung eines Ordnungswidrigkeitenverfahrens setzt zumindest einen Anfangsverdacht gem. § 46 OWiG, § 152 Abs. 2 StPO, d.h. **zureichende tatsächliche Anhaltspunkte** für das Vorliegen einer Ordnungswidrigkeit voraus. Ohne einen solchen Anfangsverdacht halte ich eine Anzeige und die Aufnahme von Ermittlungen für unzulässig.

In einem Gespräch mit dem Datenschutzbeauftragten des Bayer. Rundfunks habe ich mich dann auf folgendes Verfahren geeinigt:

Die Rundfunkbeauftragten versuchen, den Sachverhalt mit den zur Verfügung stehenden Mitteln aufzuklären. Erst wenn sich dabei Anhaltspunkte für ihre Vermutung ergeben, daß das Rundfunkgerät im Kraftfahrzeug ohne die erforderliche Anmeldung betrieben wird und deshalb eine Ordnungswidrigkeit gem. Art. 9 Abs. 1 Nr. 1 Rundfunkgebührenstaatsvertrag vorliegt, wird Anzeige erstattet. Solche konkreten Anhaltspunkte sind z.B. die wahrscheinliche Nutzung des Kraftfahrzeugs als „Geschäftswagen" und widersprüchliche oder erkennbar falsche Aussagen von Personen, die als Kfz-Halter in Frage kommen, dies aber bestreiten. Unter Darlegung solcher **konkret benannter Umstände** bestehen dann keine rechtlichen Bedenken, wenn der Rundfunk bei der Kreisverwaltungsbehörde den Antrag auf Einleitung eines Ordnungswidrigkeitenverfahrens stellt und im Laufe des Verfahrens als Beteiligter die Halterdaten erfährt.

Sollte dieser aufgezeigte Weg nicht gangbar sein, müßte überlegt werden, ob den Rundfunkanstalten zur Sicherung des Gebührenaufkommens und zur Ermittlung der Schwarzhörer durch Änderung des Straßenverkehrsgesetzes ein Auskunftsanspruch eingeräumt werden sollte.

20.3 Einheitliche Notrufnummer in Europa

Nach Plänen der Europäischen Gemeinschaft sollen bis Ende 1995 in der EG einheitliche Notrufnummern eingeführt werden. Diese einheitliche Notrufnummer soll in Deutschland die bisherigen Notrufnummern „112" für die Feuerwehr und „110" für die Polizei ersetzen. Die Notrufe sollen nach den Plänen der EG dann einheitlich bei der Polizei „auflaufen".

Die Einführung einer einheitlichen Notrufnummer wirft datenschutzrechtliche Probleme auf:

- Dürfen Anrufe, bei denen es um die Rettung von Menschenleben geht, die aber nicht mit Unfällen zusammenhängen, überhaupt bei der Polizei ankommen und dort aufgezeichnet werden?
- Dürfen diese Anrufe für polizeiliches Handeln verwendet werden?

Diese datenschutzrechtlichen Probleme bedürfen der Klärung. Sofern sich keine Lösung abzeichnet, wende ich mich mit Entschiedenheit gegen diese einheitliche Notrufnummer. Das Staatsministerium des Innern hat mir auf Anfrage versichert, bis Ende 1995 werde es bei der bisherigen Verfahrensweise bleiben. Erst danach werde die Frage entschieden werden.

20.4 Zentrales Verkehrsinformationssystem (ZEVIS)

ZEVIS ist ein zentrales Verkehrsinformationssystem, in dem ein Teil der vom Kraftfahrtbundesamt im Zentralen Fahrzeugregister und im Verkehrszentralregister gespeicherten Daten so erfaßt ist, daß bestimmte Stellen diese Daten unmittelbar (online) abrufen können. Zu diesen abrufberechtigten Stellen zählen auch bayerische Polizeidienststellen.

ZEVIS umfaßt sowohl den gesamten Bestand der in Deutschland zugelassenen Fahrzeuge als auch sog. negative Fahrerlaubnisdaten, wie z.B. Versagung oder Entziehung der Fahrerlaubnis. Rechtsgrundlage für ZEVIS sind das Straßenverkehrsgesetz (§§ 30a, 36 StVG) und die Fahrzeugregisterverordnung (§§ 12 bis 14 FRV).

In Bayern bestanden am 6.3.1991 4495 sog. virtuelle ZEVIS-Anschlüsse. Der Bundesbeauftragte für den Datenschutz hat im Hinblick auf die **Zahl** der ZEVIS-Berechtigungen der bayerischen Polizei Bedenken geltend gemacht. Diese Bedenken teile ich nicht:

Nach § 36 Abs. 5 Nr. 1 StVG ist die Einrichtung von Anlagen zum Abruf im automatisierten Verfahren zulässig, wenn nach näherer Bestimmung durch Rechtsverordnung gewährleistet ist, daß die zum Abruf bereitgehaltenen Daten der Art nach für den Empfänger erforderlich sind und ihre Übermittlung durch automatisierten Abruf unter Berücksichtigung der schutzwürdigen Belange des Betroffenen und der Aufgabe des Empfängers angemessen ist. Diese Voraussetzungen sind bei den virtuellen ZEVIS-Anschlüssen der bayerischen Polizei erfüllt. Wesentliche Aufgaben der Polizei sind nach den Bestimmungen des Polizeiaufgabengesetzes und der Strafprozeßordnung die Gefahrenabwehr und die Strafverfolgung. Jeder im Vollzugsdienst tätige Beamte ist zur Wahrnehmung der Aufgaben der Polizei im gesamten

Staatsgebiet befugt. Polizeiliche Aufgaben, die einen Abruf im automatisierten Verfahren erforderlich machen, können deshalb grundsätzlich auf jeden Polizeivollzugsbeamten zukommen. Jeder Polizeivollzugsbeamte ist deshalb nach dem Straßenverkehrsgesetz und der Fahrzeugregisterverordnung grundsätzlich befugt, von diesem Verfahren Gebrauch zu machen. Dementsprechend ist in Bayern jedes INPOL-berechtigte Endgerät gleichzeitig für ZEVIS berechtigt und kann über sog. virtuelle Terminals direkt auf ZEVIS zugreifen.

Zur Sicherung gegen Mißbrauch der Abrufmöglichkeit im Einzelfall sehen das Straßenverkehrsgesetz und die Fahrzeugregisterverordnung u.a. die Aufzeichnungen der Abrufe durch das Kraftfahrt-Bundesamt vor. In Bayern wird darüber hinaus **jeder** Abruf derart aufgezeichnet, daß die Feststellung der für den Abruf verantwortlichen Person und des Grundes der Abfrage möglich ist, also für alle Abfragen eine Zusatzprotokollierung durchgeführt wird. Bei jeder Abfrage können anhand der vollständigen Zusatzprotokollierung sowohl die Dienststelle festgestellt werden, von der aus der Abruf getätigt wurde, als auch die Dienstkraft, die den Abruf getätigt hat. Nach meiner Auffassung bietet dieses Verfahren sogar einen größeren Schutz vor Mißbrauch als die Kennung des tatsächlichen Endgerätes allein. Die Protokolldaten werden von mir auf evtl. Verstöße gegen datenschutzrechtliche Bestimmungen stichprobenartig überprüft.

Die Effektivität der vollständigen Protokollierung aller ZEVIS-Abfragen in Bayern belegt ein Vorgang, den ich nach einem Hinweis durch den Landesbeauftragten für den Datenschutz eines anderen Bundeslandes geprüft habe: Ein Bürger hatte sich an den dortigen Landesbeauftragten gewandt, weil er vermutete, daß öffentliche Stellen seine personenbezogenen Daten (Anschrift, Totalschaden bei Verkehrsunfall) unberechtigt an private Unternehmen (Autohändler) übermittelt hatten. Nach Auswertung der Protokolldaten konnte der tatsächliche Umfang von ZEVIS-Abfragen eines bestimmten Polizeibeamten festgestellt werden. Für den überwiegenden Teil der Abfragen war eine dienstliche Tätigkeit nicht ersichtlich. Strafrechtliche Ermittlungen gegen den Beamten sind eingeleitet.

Bei mehreren Polizeidirektionen habe ich stichprobenartig ZEVIS-Abfragen durch Auswertungen der beim Bayer. Landeskriminalamt geführten **Protokolldatei überprüft.** In allen Fällen konnte der den ZEVIS-Abfragen zugrundeliegende Sachverhalt und die Berechtigung zur Abfrage festgestellt werden. Die Überprüfung hatte am Tag nach dem vorgesehenen Stichtag begonnen, so daß sich die Polizeibeamten noch gut an die Abfragen erinnern konnten.

Aufgrund von Beschlüssen des Bundestags und des Bundesrats hat der Bundesminister für Verkehr einen Erfahrungsbericht über ZEVIS erstellt. Der Bundesbeauftragte für den Datenschutz, der an der Erarbeitung des Berichts beteiligt war, hat eine Reihe von Forderungen aufgestellt, die ich zum Teil nicht unterstützen kann:

- Der Anlaß eines Abrufs aus ZEVIS ist von der abrufenden Stelle (z.B. Polizei) durch die Angabe von sog. Schlüsselzahlen zu begründen. Derzeit sieht die FRV sechs Schlüsselzahlen (z.B. Schlüsselzahl 5: Verfolgung von Straftaten oder Verkehrsordnungswidrigkeiten) vor. Der Bundesbeauftragte für den Datenschutz fordert eine Erweiterung auf zehn Schlüsselzahlen.

  Mit einer weiteren Aufschlüsselung des Abfragegrundes läßt sich zwar theoretisch eine genauere Begründung der einzelnen Abfragen erreichen. Ich habe jedoch erhebliche Zweifel, ob durch eine Erhöhung der Schlüsselzahlen die Kontrolle der Zulässigkeit der getätigten Abrufe tatsächlich verbessert wird. Bei einer datenschutzrechtlichen Prüfung der Abfragen und der Verwendung der bisherigen sechs Schlüsselzahlen bei ZEVIS-Abfragen hat sich ergeben, daß die sechs Schlüsselzahlen völlig ausreichend sind. Bei meinen Kontrollen der protokollierten ZEVIS-Abfragen haben sich in keinem Fall Probleme bei der Prüfung der einzelnen Abfragen ergeben. Zu jedem geprüften Fall ließen sich der Sachverhalt und der Anlaß der Abfrage nachvollziehen.

  Die Verwendung von 10 statt bisher 6 Schlüsselzahlen dürfte kaum die Nachprüfbarkeit der Abfragen verbessern, wohl aber die Zahl der formalen Fehler durch Verwechslung der Schlüsselzahlen erhöhen.

- ZEVIS enthält bisher nur sog. negative Fahrerlaubnisdaten (Versagung und Entziehung der Fahrerlaubnis). Die Beschränkung der Abrufe auf diese Daten wird von der Polizei kritisiert, da mit Hilfe dieser Speicherungen nicht festgestellt werden könne, ob eine Person tatsächlich und rechtmäßig im Besitz einer Fahrerlaubnis ist.

  Der Bundesbeauftragte für den Datenschutz hält die Schaffung eines neuen Fahrerlaubnisregisters nicht für erforderlich und verneint die Notwendigkeit, darin enthaltene Informationen für Verkehrskontrollen zum Online-Abruf bereitzuhalten.

  Demgegenüber ist nach meiner Auffassung ein automatisiertes zentrales Verzeichnis aller Führerscheininhaber für die Vollzugspolizei ein nützliches und notwendiges Instrument zur zuverlässigen Feststellung der Fahrerlaubnis und damit zur Gewährleistung der Verkehrssicherheit. Eine Beeinträchtigung des Persönlichkeitsrechts durch die

Speicherung des positiven Datums der Fahrerlaubnis vermag ich nicht zu erkennen.

- Personenbezogene Anfragen in ZEVIS werden in einer Datei protokolliert. Diese Aufzeichnungen dürfen nach den gesetzlichen Bestimmungen nur zur Kontrolle der Zulässigkeit der Abrufe verwertet werden und sind durch geeignete Vorkehrungen gegen zweckfremde Nutzung und gegen sonstigen Mißbrauch zu schützen; sie sind nach drei Monaten zu löschen, es sei denn, die Aufzeichnungen werden noch bis zum Abschluß eines bereits eingeleiteten Kontrollverfahrens benötigt.

Der Bundesbeauftragte für den Datenschutz ist der Auffassung, daß eine Nutzung der Protokolldaten zu anderen Zwecken als zur Datenschutzkontrolle aus datenschutzrechtlicher Sicht grundsätzlich nicht zugelassen werden sollte. Die nur für Kontrollzwecke geschaffenen Datensammlungen sollten auch nur diesem Zweck dienen und müßten gegen jegliche Zweckentfremdung geschützt werden.

Diese Forderung hat zwar im Straßenverkehrsgesetz ihren Niederschlag gefunden. Die Regelung sollte gleichwohl überdacht werden. Es gibt keine überzeugenden Gründe, die Nutzung von Protokolldaten selbst zur Aufklärung von Verbrechen zu verhindern. Deshalb sieht Art. 46 Abs. 3 PAG vor, daß Protokollbestände, die nach Abfragen im automatisierten Abrufverfahren eingerichtet worden sind, zu Zwecken der Kriminalitätsbekämpfung und der Datensicherung ausgewertet werden dürfen. Deshalb sollte durch eine entsprechende Änderung des Straßenverkehrsgesetzes die Voraussetzungen für die Nutzung der Protokolldatei zur Verbrechensbekämpfung unter Auflagen, die die datenschutzrechtlichen aber auch polizeilichen Bedürfnisse berücksichtigen, geschaffen werden.

Nach der Errichtungsanordnung für die beim Landeskriminalamt eingerichteten Protokolldatei für alle Online-Abfragen ist in Bayern die Auswertung des Datenbestandes u.a. für Zwecke der Verbrechensbekämpfung zulässig, wenn dies zur Aufklärung oder Verfolgung bestimmter Straftaten erforderlich ist. Die protokollierten Daten werden für die Dauer von 12 Monaten gespeichert. Auf meine Forderung hat das Innenministerium sichergestellt, daß ZEVIS-Protokolldaten von der Nutzung zur Verbrechensbekämpfung ausgenommen sind und für sie die Auswertungsbeschränkungen des Straßenverkehrsgesetzes und der Fahrzeugregisterverordnung maßgebend sind.

21. Medien

21.1 Medien und Datenschutz

Im Berichtszeitraum habe ich erneut auf den unzureichenden Persönlichkeitsschutz gegenüber Rundfunk, Presse und Film hingewiesen: ein hinreichender Schutz des Persönlichkeitsrechts des Bürgers ist nur dann gewährleistet, wenn dem Betroffenen schon vor einer rechtsverletzenden Berichterstattung **vorbeugende** Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsansprüche zustehen und eine hinreichende Datenschutzkontrolle durch ein unabhängiges Kontrollorgan sichergestellt ist. Die im Berichtszeitraum in Kraft getretenen oder im Entwurf vorgelegten Gesetze und Staatsverträge für den Medienbereich weisen überwiegend erfreuliche Fortschritte in Richtung einer Verbesserung des Datenschutzes auf, wenn auch meine Forderungen nicht in vollem Umfang erfüllt worden sind.

21.2 Rundfunkanstalten des Bundes

Die Datenschutzregelungen für die Rundfunkanstalten des Bundes finden sich im Bundesdatenschutzgesetz (BDSG), welches am 01.06.1991 in Kraft getreten ist. Erstmals im Rundfunkbereich werden die Rundfunkanstalten des Bundes verpflichtet, bei Veröffentlichung von Gegendarstellungen des Betroffenen diese zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst. Derjenige, der durch eine Berichterstattung der Rundfunkanstalten des Bundes in seinem Persönlichkeitsrecht beeinträchtigt wird, kann Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten sowie die Berichtigung unrichtiger Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Für die Überwachung des Datenschutzes bei den Rundfunkanstalten des Bundes ist die Bestellung eines Beauftragten für den Datenschutz bei den Rundfunkanstalten vorgesehen, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt und in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist.

21.3 Datenschutz bei der Presse

Für den Bereich der Presse schreibt das Bundesdatenschutzgesetz für den journalistisch-redaktionellen Teil lediglich die Beachtung des Datengeheimnisses und technisch-organisatorische Maßnahmen zur Gewährleistung der Datensicherheit vor. **Weitergehende Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsansprüche werden den von der Datenverarbeitung Betroffenen vorenthalten.** Während sich im übrigen Medienbereich im Zuge der abgeschlossenen oder beabsichtigten Novellierungen der Datenschutz-

gesetze bzw. der Rundfunkstaatsverträge deutliche Verbesserungen des Datenschutzes abzeichnen, sind solche Verbesserungen bei der Presse nahezu völlig ausgeblieben, obwohl das Bedürfnis nach Datenschutz hier keinesfalls geringer ist als beim Rundfunk. Auch für diesen Bereich ist zu fordern, daß der Gesetzgeber die erforderlichen Regelungen zum Schutz des Persönlichkeitsrechts erläßt. Da der Bund nach Art. 75 Nr. 2 Grundgesetz eine Rahmengesetzgebungskompetenz für diesen Bereich besitzt, sollte er die erforderlichen Regelungen in einem Bundes-Presserechtsrahmengesetz treffen. Auch eine Ergänzung des Bundesdatenschutzgesetzes wäre möglich. Solange der Bund keine abschließende Regelungen trifft, wären die Länder von der verfassungsrechtlichen Kompetenzlage her nicht gehindert, geeignete Datenschutzregelungen in Landesgesetzen zu treffen. Eine Regelung auf Bundesebene wäre jedoch wegen der über die Landesgrenzen hinausgehenden Verflechtung des Medienmarkts vorzuziehen. Im Interesse der Wettbewerbsgleichheit ist zu hoffen, daß der Bundesgesetzgeber die Presse alsbald mit dem Rundfunk gleichstellt.

21.4 Bayerischer Rundfunk

Die Regelung des Datenschutzes bei den Landesrundfunkanstalten ist Angelegenheit der Länder. Der Datenschutz im Bereich des Bayer. Rundfunks ist im Bayer. Datenschutzgesetz nur ansatzweise geregelt. Werden personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeitet, so ist lediglich die Vorschrift über technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu beachten: ein Datenschutzbeauftragter des Bayer. Rundfunks wacht über die Einhaltung dieses Datenschutzes. Das Bayer. Datenschutzgesetz gewährt dem von der Datenverarbeitung des Bayer. Rundfunks Betroffenen insbesondere keine Ansprüche, um eine Beeinträchtigung seines Persönlichkeitsrechts durch die Datenverarbeitung zu verhindern. Diese Ansprüche müssen im neuen Bayer. Datenschutzgesetz oder in einem neuen Gesetz über den Bayer. Rundfunk geschaffen werden.

21.5 Entwurf des Bayerischen Mediengesetzes

Der private Rundfunk in Bayern ist bislang im Bayer. Medienerprobungs- und -entwicklungsgesetz (MEG) geregelt. Dieses Gesetz, das Grundlage für die Gestaltung privater Rundfunkangebote unter der öffentlich-rechtlichen Trägerschaft der Bayer. Landeszentrale für Neue Medien ist, tritt spätestens am 1. Dezember 1992 außer Kraft. Es soll abgelöst werden durch das Bayer. Mediengesetz (BayMG). Der Gesetzentwurf der Staatsregierung enthält Datenschutzregelungen, die über die bisherigen Regelungen des MEG hinausgehen. Viele datenschutzrechtliche Forderungen, die ich zu einem Vorentwurf erhoben habe, sind in dem neuen Entwurf berücksichtigt:

- Die **Gegendarstellung** einer Person oder Stelle, die durch eine in einer Rundfunksendung aufgestellte Tatsachenbehauptung betroffen ist, ist vom Anbieter dieser Sendung auf seine Kosten zu verbreiten. Gegendarstellungen sind zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.
- Schutz der anfallenden Verbindungs- und Abrechnungsdaten gemäß den Bestimmungen des Rundfunkstaatsvertrags.
- Wird jemand durch eine Sendung in seinem Persönlichkeitsrecht beeinträchtigt, so kann er vom Anbieter **Auskunft** über die der Sendung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die **Berichtigung** unrichtiger Daten verlangen. Im übrigen gelten für die ausschließlich zu eigenen journalistisch-redaktionellen Zwecken erfolgende Verarbeitung oder Nutzung personenbezogener Daten nur die Vorschriften über das Datengeheimnis und technische und organisatorische Maßnahmen des Bayer. Datenschutzgesetzes.
- Die Überwachung der Einhaltung der Datenschutzvorschriften bei der Landeszentrale für Neue Medien, den Medienbetriebsgesellschaften, den Betreibern von Kabelanlagen, ausgenommen die Deutsche Bundespost, und bei den Anbietern gehörte bisher zu meinen Aufgaben. Sie soll nach dem Entwurf auf einen unabhängigen Beauftragten für den Datenschutz bei der Landeszentrale übertragen werden. Jedermann kann sich an den Beauftragten wenden mit dem Vorbringen, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein. Der Beauftragte übermittelt seine Berichte, die er mindestens alle 2 Jahre zu erstatten hat, auch dem Landesbeauftragten für den Datenschutz.
- Im übrigen sind für die Landeszentrale, für die Medienbetriebsgesellschaften, für die Betreiber von Kabelanlagen mit Ausnahme der Deutschen Bundespost und für die Anbieter die jeweils geltenden Vorschriften über den Schutz personenbezogener Daten anzuwenden, auch wenn die Daten nicht in Dateien verarbeitet und genutzt werden.

Ich habe zur weiteren Verbesserung des Datenschutzes vorgeschlagen, über den vorgesehenen Auskunfts- und Berichtigungsanspruch hinaus auch einen Anspruch auf Sperrung unrichtiger Daten vorzusehen, wenn die richtigen Daten nicht festgestellt werden können und deshalb eine Berichtigung nicht möglich ist. Darüber hinaus halte ich auch für den Geltungsbereich des Bayer. Mediengesetzes zur Ge-

währleistung eines ausreichenden Schutzes des Persönlichkeitsrechts **Auskunftsansprüche der Betroffenen schon vor einer Rechtsbeeinträchtigung** für unbedingt erforderlich. Berichtigungs- und Sperrungsansprüche entfalten nur dann ihre volle Wirksamkeit, wenn der Betroffene bereits vor einer Beeinträchtigung des Persönlichkeitsrechts Auskunft erhalten und seine Rechte geltend machen kann.

21.6 Staatsvertrag über den Rundfunk im vereinten Deutschland

Die Regierungschefs der alten und neuen Länder haben am 31. August 1991 den Staatsvertrag über den Rundfunk im vereinten Deutschland abgeschlossen. Ziel dieses Staatsvertrages ist es, ein in den alten und den neuen Ländern gleichermaßen geltendes staatsvertragliches Rundfunkrecht zu schaffen. Er besteht aus einem allgemeinen Teil, dem Rundfunkstaatsvertrag, der dem öffentlich-rechtlichen und privaten Rundfunksystem in der Bundesrepublik Deutschland eine Rahmenordnung geben will. Er stellt u.a. klar, daß das jeweilige Landesrecht anwendbar bleibt, soweit keine anderslautenden Regelungen im Staatsvertrag bestehen. Darüber hinaus enthalten weitere Artikel des Staatsvertrages als besondere Vorschriften den ARD-Staatsvertrag, ZDF-Staatsvertrag, Rundfunkgebühren-Staatsvertrag, Rundfunkfinanzierungs-Staatsvertrag sowie den Bildschirmtext-Staatsvertrag. Die Neuregelungen des Datenschutzrechts enthalten deutliche Verbesserungen des Datenschutzes, wenn auch hier die Einräumung eines vorbeugenden Rechtsschutzes nicht erreicht werden konnte. Dies gilt insbesondere für folgende Verträge:

Der **Rundfunkstaatsvertrag** regelt in § 28 die Verarbeitung personenbezogener Daten über die Inanspruchnahme einzelner Programmangebote. Der Rundfunkteilnehmer, Hörer wie Zuschauer, soll die Gewähr haben, daß seine Benutzergewohnheiten nicht ausgeforscht und zu seinem Nachteil ausgenutzt werden. Daten dürfen nur erhoben, verarbeitet und genutzt werden, soweit und solange dies erforderlich ist, um den Abruf von Programmangeboten zu vermitteln (Verbindungsdaten), oder die Abrechnung der Entgelte zu ermöglichen, die der Teilnehmer für die Inanspruchnahme der technischen Einrichtungen und Programmangebote zu entrichten hat (Abrechnungsdaten). Zur Speicherung der Abrechnungsdaten ist bestimmt, daß sie Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter vom einzelnen Teilnehmer in Anspruch genommener Programmangebote nicht erkennen lassen darf, es sei denn, der Teilnehmer beantragt schriftlich eine nach einzelnen Programmangeboten aufgeschlüsselte Abrechnung der Entgelte. Die Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte ist nicht zulässig, es sei denn, Abrechnungsdaten werden an den Rundfunkveranstalter zum Zwecke der Einziehung einer Forderung übermittelt, wenn diese auch nach Mahnung nicht beglichen wird. Abrechnungsdaten sind zu löschen, sobald sie für Zwecke der Abrechnung nicht mehr erforderlich sind. Verbindungsdaten sind nach dem Ende der jeweiligen Verbindung zu löschen. Darüber hinaus werden technische und organisatorische Schutzmaßnahmen zur Einhaltung der vorgenannten Pflichten und zur Gewährleistung der Datensicherheit vorgeschrieben.

Der **ZDF-Staatsvertrag** enthält eigene Datenschutzvorschriften. Soweit personenbezogene Daten durch das ZDF ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet werden, gelten die für das Datengeheimnis und für die Datensicherung maßgeblichen Vorschriften des Rheinland-Pfälzischen Datenschutzgesetzes. Führt die journalistisch-redaktionelle Verwendung personenbezogener Daten zur Verbreitung von **Gegendarstellungen** des Betroffenen, so sind diese zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln. Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht **beeinträchtigt**, kann der Betroffene **Auskunft** über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, oder auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann, oder durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe des ZDF durch Ausforschung des Informationsbestandes beeinträchtigt würde. Der Betroffene kann die **Berichtigung** unrichtiger Daten oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Das ZDF bestellt einen **unabhängigen Beauftragten für den Datenschutz**, der an die Stelle des Landesbeauftragten für den Datenschutz tritt und die Einhaltung des Datenschutzes beim ZDF überwacht. Jedermann hat das Recht, sich unmittelbar an den Beauftragten für den Datenschutz zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch das ZDF in seinen schutzwürdigen Belangen verletzt zu sein.

Der **Rundfunkgebührenstaatsvertrag** ist die Grundlage für einen einheitlichen Gebühreneinzug in Deutschland. In ihm wurden bereichsspezifische Datenschutzregelungen für den Rundfunkgebühreneinzug verankert. Er enthält die Verpflichtung des Rundfunkteilnehmers, Beginn und Ende des Bereithaltens eines Rundfunkempfangsgeräts zum Empfang unverzüglich der Landesrundfunkanstalt anzuzeigen. Dabei hat der Teilnehmer eine Reihe personenbezoge-

ner Daten mitzuteilen und auf Verlangen nachzuweisen, wie etwa Name, Geburtsdatum, Anschrift sowie Angaben über das Bereithalten von Rundfunkempfangsgeräten. Diese Daten des Rundfunkteilnehmers darf die Landesrundfunkanstalt nur für die ihr im Rahmen des Rundfunkgebühreneinzugs obliegenden Aufgaben verarbeiten und nutzen.

Vom Rundfunkteilnehmer, bei dem tatsächliche Anhaltspunkte vorliegen, daß er ein Rundfunkempfangsgerät zum Empfang bereithält und es nicht oder nicht umfassend angezeigt hat, kann die Landesrundfunkanstalt Auskünfte über diejenigen Tatsachen verlangen, die Grund, Höhe und Zeitraum der Gebührenpflicht betreffen. Es ist die Befugnis für die Rundfunkanstalt vorgesehen, im Einzelfall weitere Daten zu erheben, soweit dies jeweils erforderlich ist, um das Vorliegen der Gebührenpflicht zu beurteilen. Soweit Anhaltspunkte vorliegen, daß ein Empfangsgerät zum Empfang bereitgehalten wird und dies nicht ordnungsgemäß angezeigt wurde, dürfen die Landesrundfunkanstalten auch Auskünfte bei den Meldebehörden einholen, soweit dies zur Überwachung der Rundfunkgebührenpflicht erforderlich ist und die Erhebung der Daten beim Betroffenen nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Die getroffenen Regelungen halte ich für erforderlich und sachgerecht, da gewährleistet werden muß, daß der gebührenpflichtige Personenkreis erfaßt werden kann. Dabei ist der Auskunftsanspruch hinreichend beschränkt, da er nur eingreift, wenn tatsächliche Anhaltspunkte vorliegen, daß der Verpflichtung zur Anzeige durch den Rundfunkteilnehmer nicht ausreichend nachgekommen wurde. Damit ist das Auskunftsrecht sowohl Bezug auf die Adressaten als auch dem Gegenstand nach ausreichend konkretisiert und begrenzt.

21.7 Prüfung einer Kabelgesellschaft

Im Berichtszeitraum wurde eine zweite örtliche Kabelgesellschaft datenschutzrechtlich überprüft, für deren Kontrolle ich nach dem Medienerprobungsgesetz zuständig bin. Die Kabelgesellschaften produzieren selbst keine Rundfunkprogramme. Sie organisieren lediglich die privaten Rundfunkangebote und stellen aus den eigengestalteten Beiträgen der Anbieter Rundfunkprogramme zusammen und sorgen für ihre Verbreitung. Sie stellen die notwendigen technischen Einrichtungen wie Studiotechnik und Übertragungswagen zur Verfügung.

Bei der Prüfung habe ich folgende Feststellungen getroffen:

Eine **automatisierte Datenverarbeitung** findet bei der geprüften Kabelgesellschaft nicht statt. Sämtliche Geschäftsunterlagen werden in Aktenordnern abgelegt und in Aktenschränken verwahrt. Während ein kleinerer Aktenschrank abschließbar ist, befinden sich die meisten Unterlagen über die Rundfunkteilnehmer in einem neu angeschafften, **nicht abschließbaren Aktenschrank**. Im Büro eines Geschäftsführers im Rathaus der Stadt befindet sich ein weiterer kleiner Teil von Unterlagen über die Rundfunkteilnehmer. Die Unterbringung in nicht verschließbaren Schränken genügt nicht den datenschutzrechtlichen Mindestanforderungen (Art. 15 BayDSG). Aus Gründen der Datensicherheit kann diese Aufbewahrung nur hingenommen werden, wenn die Kabelgesellschaft dafür Sorge trägt, daß ein unbeaufsichtigtes Betreten der Geschäftsräume von dritten Personen ausgeschlossen werden kann. Hinsichtlich der im städtischen Rathaus verwahrten Unterlagen habe ich gefordert, diese möglichst bald in die Geschäftsräume der Kabelgesellschaft zu überführen.

Bei den vorgenannten Unterlagen über die Rundfunkteilnehmer handelt es sich um von der Deutschen Bundespost übermittelte Aufträge für Kabelanschlüsse, um Änderungsmitteilungen bei Umzug oder Ausscheiden von Teilnehmern. Ferner finden sich hier sonstige Mitteilungen, wie die Feststellung eines Schwarzanschlusses. Diese Datenübermittlung der Post ist unbedenklich, da von ihr Teilnehmer gemeldet werden, die neben einem fernmelderechtlichen Vertrag auch mit der Kabelgesellschaft rundfunkrechtliche Teilnehmerverträge abschließen. Der Einzug der den Kabelgesellschaften zustehenden Teilnehmerentgelte wird derzeit noch von der Deutschen Bundespost durchgeführt (Art. 23 Abs. 3 Satz 3 MEG). Die Datenübermittlung dient somit dem Nachweis der entgeltpflichtigen Teilnehmer gegenüber der Kabelgesellschaft.

Die **Form der Verwaltung** der Teilnehmerdaten entspricht nicht den datenschutzrechtlichen Anforderungen. Alle Unterlagen von Teilnehmern, welche die Deutsche Bundespost an die Kabelgesellschaft übersendet, werden, sortiert nach dem Wohnsitz, in der Reihenfolge des Eingangs nacheinander abgeheftet. Eine alphabetische Ordnung der Daten nach den Namen der Teilnehmer erfolgt nicht. Entsprechend werden auch eingehende Änderungsmitteilungen nicht bei den betreffenden Anmeldungen abgeheftet. Unterlagen eines einzelnen Teilnehmers befinden sich deshalb an verschiedenen Stellen des Ordners. Das Zusammenführen aller Teilnehmerdaten ist nur bei Durchsicht des gesamten Ordners möglich. Die Feststellung des aktuellen Datenbestandes und die zutreffende Datenbeurteilung sind dadurch erschwert. So ist es zum Beispiel denkbar, daß eine Person als „Schwarzseher" im Akt erscheint, ohne daß ein in diesem Fall zwischenzeitlich längst erfolgter ordnungsgemäßer Anschluß an das Kabelnetz im Zusammenhang ersichtlich ist. Auch befinden sich in den Ordnern Unterlagen über Teilnehmer, die längst ausgeschieden sind. Eine Aussonderung oder Ver-

nichtung von Unterlagen hat bislang noch nicht stattgefunden.

Diese Datenverwaltung widerspricht auch Art. 19 Abs. 1 des Medienerprobungs- und -entwicklungsgesetzes (MEG), wonach personenbezogene Daten zu löschen sind, sobald sie für das Erbringen einer Leistung, für den Abschluß oder die Abwicklung eines Vertrags mit dem Teilnehmer, die Erreichung des Vertragszwecks oder Zwecke der wissenschaftlichen Begleitforschung im Rahmen des MEG nicht mehr benötigt werden. Dieser Zustand kann allenfalls noch für eine Übergangszeit hingenommen werden, bis die Frage des künftigen Einzugs der Teilnehmerentgelte abschließend geklärt ist. Zur Zeit wird der Gebühreneinzug durch eine neu gegründete Medien-Service-GmbH vorbereitet. Sobald die Fragen des künftigen Inkassos und des dabei anfallenden Datenbedarfs geklärt sind, müssen auch der weitere Verbleib der Teilnehmerdaten, ihre Aktualisierung sowie die Aussonderung und Vernichtung von nicht weiter benötigten Daten geklärt und gelöst werden.

21.8 Datenschutz in der Telekommunikation

Am 1. Juli 1991 trat die Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TELEKOM-Datenschutzverordnung — TDSV) in Kraft. Die Verordnung löste damit die bisherigen im Fernmeldeverkehr geltenden Datenschutzbestimmungen der Telekommunikationsordnung (TKO) ab, die mit Ablauf des 30. Juni 1991 außer Kraft trat. Die TDSV gilt für die Fernmeldedienstleistungen (z.B. Telefon, Telex, Datenübertragung, Bildschirmtext usw.) der Deutschen Bundespost TELEKOM und enthält bereichsspezifische Regelungen für den Umgang mit den bei der Erbringung von Telekommunikationsdienstleistungen anfallenden personenbezogenen Daten der am Fernmeldeverkehr Beteiligten.

Viele — wenn auch nicht alle — datenschutzrechtlichen Forderungen, die im Zusammenhang mit der Einführung des dienste-integrierenden digitalen Fernmeldenetzes ISDN erhoben worden sind, sind in der TDSV berücksichtigt. Die TDSV enthält insbesondere folgende Regelungen für den Umgang mit personenbezogenen Daten:

- Nach Beendigung der Verbindung werden aus den Verbindungsdaten (z.B. Rufnummer oder Kennung des anrufenden und des angerufenen Anschlusses) unverzüglich die für die Berechnung des Entgelts erforderlichen Daten ermittelt. Spätestens mit Versendung der Entgeltrechnung werden die Verbindungsdaten in Sprachkommunikationsdiensten nach Wahl des entgeltpflichtigen Kunden vollständig gelöscht oder unter Verkürzung der Zielnummer um die letzten 3 Ziffern gespeichert oder vollständig gespeichert, wenn ein Einzelentgeltnachweis beantragt wurde. Diese Wahlmöglichkeit gilt jedoch erst dann, wenn die erforderlichen Datenverarbeitungsprogramme verfügbar sind, spätestens aber ab 1. Juli 1992. Bis dahin werden die Verbindungsdaten, wie in allen anderen Telekommunikationsdiensten, vollständig gespeichert.

- Soweit die Verbindungsdaten auf Wunsch gespeichert bleiben, werden sie 80 Tage nach Versendung der Entgeltrechnung gelöscht.

- Auf Antrag wird dem Kunden ein entgeltpflichtiger Einzelentgeltnachweis mit den nach seiner Wahl verkürzt oder vollständig gespeicherten Zielnummern erteilt. Bei stationären Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn alle zum Haushalt gehörenden Mitbenutzer des Anschlusses sich mit der Bekanntgabe der Verbindungen schriftlich einverstanden erklärt haben.

- Der Anruf bei Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz ober überwiegend über Telefon abwickeln, darf aus dem Nachweis nicht ersichtlich sein. Hierzu gehören neben den in § 203 Abs. 1 Nr. 4 und Nr. 4 a des Strafgesetzbuches genannten Personengruppen insbesondere Telefonseelsorge und Gesundheitsberatung. Die Deutsche Bundespost TELEKOM ist auf Antrag einer solchen Person, Behörde oder Organisation verpflichtet, durch technische Vorrichtungen die Beachtung dieser Vorschrift sicherzustellen. Diese Vorschrift tritt jedoch erst in Kraft, sobald die zu ihrer Durchführung erforderlichen Datenverarbeitungsprogramme verfügbar sind, spätestens am 1. Juli 1992.

- Werden Anschlüsse angeboten, die die Rufnummer des Anrufenden an den angerufenen Anschluß übermitteln, ist dem Kunden eine Wahlmöglichkeit zwischen der Anzeige seiner Rufnummer bei jedem Anruf oder dem dauernden Ausschluß der Anzeige seiner Rufnummer einzuräumen. Die Möglichkeit einer fallweisen Unterdrükkung der Übermittlung der Rufnummer des anrufenden an den angerufenen Anschluß ist spätestens ab 1. Januar 1994 vorzusehen.

- Für Sprachkommunikationsdienste ist auf Antrag die Übermittlung der Rufnummer des anrufenden Anschlusses an den angerufenen Anschluß einer der oben genannten Beratungsstellen in der Vermittlungsstelle dieses Anschlusses auszuschließen. Auf Antrag sind Anschlüsse bereitzustellen, zu denen eine Übermittlung der Rufnummer des anrufenden Anschlusses an den angerufenen Anschluß ausgeschlossen ist. Diese Anschlüsse sind auf Antrag des Kunden in dem öffentlichen Kundenver-

zeichnis (Telefonbuch) entsprechend zu kennzeichnen.

- Auf Verlangen des Kunden muß die Eintragung in öffentliche Kundenverzeichnisse (Telefonbuch) ganz oder teilweise unterbleiben.

Weitere wichtige datenschutzrechtliche Forderungen sind in der TDSV nicht berücksichtigt:

- Zur Gebührenabrechnung sollten von der TELEKOM nur diejenigen Kundendaten gespeichert werden, die zur Berechnung der Telefongebühren in Summenform unerläßlich sind. Das heißt: Wie bisher sollte nur die jeweils aufaddierte Gebührensumme gespeichert und in der Telefonrechnung enthalten sein. Lediglich auf Antrag des Kunden dürfte zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung des Einzelgebührennachweises die Rufnummer des Angerufenen in einer zumindest um die letzten 4 Ziffern verkürzten Form gespeichert werden. Diese Daten sollten spätestens 80 Tage nach dem Absenden der Entgeltrechnung gelöscht werden. Die in der Verordnung vorgesehene Möglichkeit der vollständigen Speicherung der Zielnummer und deren Aufnahme in den Einzelentgeltnachweis sind abzulehnen.

- Verlangt der Kunde die vollständige Löschung der Verbindungsdaten, so sollten diese gelöscht werden, sobald die Berechnung der Telefongebühren durchgeführt ist. Der in der Verordnung vorgesehene Löschungszeitpunkt „spätestens mit Versendung der Entgeltrechnung" kann eine erheblich längere Speicherungsdauer bedeuten.

- Die Rufnummern der angerufenen Beratungsstellen, die auf ihren Antrag nicht im Einzelentgeltnachweis erscheinen dürfen (siehe oben), können nach der TDSV bei der TELEKOM bis zum Versenden der Gebührenrechnung in vollständiger Form gespeichert und erst anschließend gelöscht oder — nach Wahl des entgeltpflichtigen Kunden — weitere 80 Tage verkürzt oder vollständig gespeichert werden. Die Rufnummern dieser Beratungsstellen sollten nur für den zur Entgeltberechnung unbedingt notwendigen Zeitraum gespeichert werden.

Telekommunikationsdienstleistungen können künftig nicht nur von der Deutschen Bundespost TELEKOM, sondern auch von Privaten erbracht werden. Zu nennen wäre etwa der Betrieb von Satellitenfunkanlagen wie auch die Mobilfunkkommunikation. Den Schutz personenbezogener Daten in diesem Bereich soll die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Teledienstunternehmen-Datenschutzverordnung — UDSV) regeln, die bisher erst im Entwurf vorliegt. Im Entwurf der UDSV werden die in der TDSV enthaltenen unzureichenden Datenschutzregelungen übernommen.

Der Bundesrat hat am 27. September 1991 beschlossen, der UDSV nach Maßgabe insbesondere der folgenden Änderung zuzustimmen: Privilegierte Beratungsorganisationen sollen sofort ab Geltung der Verordnung auf dem Einzelentgeltnachweis nicht erscheinen und nicht erst nach einer Übergangsfrist. Zugleich forderte der Bundesrat in einer Entschließung die Bundesregierung auf, die TELEKOM-Datenschutzverordnung (TDSV) den für die UDSV vorgeschlagenen Änderungen anzupassen.

Nach § 12 des Gesetzes über Fernmeldeanlagen (FAG) kann in strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet oder für ihn bestimmt waren oder von ihm herrührten, und die Auskunft für die Untersuchung Bedeutung hat. Durch die mit der neuen Telekommunikationstechnik verbundene erweiterte Datenspeicherung sowie durch die Schaffung neuer Telekommunikationsdienste wird der Anwendungsbereich des § 12 FAG erheblich ausgedehnt. Damit erlangt die Regelung des § 12 FAG eine neue Qualität.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat in einer Entschließung vom 08. März 1991 u.a. gefordert, Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung — schon aus Gründen der Normenklarheit — in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden. Dieser Forderung hat sich auch der Bundesrat in der o.g. Entschließung angeschlossen und die Bundesregierung aufgefordert, einen Entwurf zur Änderung von § 12 FAG einzubringen, mit dem eine hinreichend bestimmte Rechtsgrundlage für die Übermittlung der personenbezogenen Daten geschaffen wird, die im Fernmeldeverkehr insbesondere nach Einführung der neuen Techniken anfallen und die von den Organen der Strafverfolgung angefordert werden können.

22. Technischer und organisatorischer Bereich

22.1 Fortentwicklung der Datensicherheit

22.1.1 Anforderungen an sichere DV-Systeme

Wegen der Abhängigkeit von dem Funktionieren der automatisierten Datenverarbeitung fordern die Anwender von den Herstellern von Datenverarbeitungssystemen höhere Sicherheit als früher.

Die Sicherheit eines Datenverarbeitungssystems hängt wesentlich ab von der eingesetzten Hardware, vom Betriebssystem und von der systemnahen Software. Das Betriebssystem ist die Summe aller Systemprogramme, die für den Betrieb eine DV-Anlage einschließlich der angeschlossenen peripheren Geräte erforderlich sind. Der höchste Sicherheitsstandard wird dabei erreicht, wenn die Sicherheitseinrichtungen im Betriebssystem integriert sind. Wenn hingegen fehlende oder unzureichende Sicherheitskomponenten eines Betriebssystems durch Zusatzprodukte ersetzt werden müssen, entstehen meist Bruchstellen, die sich zu Schwachpunkten im gesamten Sicherheitssystem entwickeln können. Sowohl in den Vereinigten Staaten von Amerika als auch in Deutschland und neuerdings auch in der Europäischen Gemeinschaft hat man durch die Festlegung von sogenannten IT-Sicherheitskriterien (IT = Informationstechnik) und die Einsetzung von Prüfinstanzen Anstrengungen unternommen, die Sicherheit von IT-Systemen zu erhöhen.

In Deutschland ist für die Prüfung und Einstufung von IT-Systemen das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig (siehe 12. Tätigkeitsbericht, Seite 61). Die vom BSI aufgestellten Sicherheitskriterien orientieren sich an den 3 Grundbedrohungen: dem Verlust der Vertraulichkeit von Daten, dem Verlust der Verfügbarkeit von Daten und dem Verlust der Integrität von Daten. Daraus ergeben sich die an IT-Systeme gestellten Sicherheitsanforderungen, die

- die Funktionalität, die sogenannte F-Klasse, und
- die Qualität und Vertrauenswürdigkeit, die sogenannte Q-Klasse,

festlegen.

Genügt ein System beispielsweise der Klasse F2/Q2, muß es folgende Funktionen unterstützen:

- Schutz des Speichers
- geschützte Wiederverwendung von Ressourcen (Löschen der Information bei der Freigabe)
- Identifikation und Authentifizierung des Benutzers
- benutzerbestimmbarer Zugriffsschutz für Objekte
- abgestufte Privilegien
- Protokollierung und Auswertung der Protokolldaten

Wegen der Komplexität der Großrechnersysteme erfordert eine solche Prüfung einen beträchtlichen Aufwand. Das BSI hat 1990 beispielsweise mit der Prüfung eines Großrechnerbetriebssystem nach F2/Q3 begonnen.

Von der Anwender- und vor allem von der Revisionsseite gibt es eine Reihe von Anforderungen an ein Großrechnerbetriebssystem. Im einzelnen handelt es sich dabei um folgende Funktionen:

Identifikation und Authentifizierung

- Das Betriebssystem muß über ein sicheres Identifikations- und Authentifizierungsverfahren verfügen (mehrstufige Kontrollen).
- Auch bei der Kommunikation in einem offenen System müssen alle Partner als berechtigt authentifiziert werden können.
- Der Zugriffschutz muß benutzerbezogen und möglichst flexibel gestaltet werden können.
- Die Speicherung der Informationen über die Zugriffsberechtigungen muß so erfolgen, daß sie auch für den Systemverwalter nicht im Klartext interpretierbar sind (Verschlüsselung).

Abgestufte Privilegien

- Die Systemverwalterprivilegien müssen auf mehrere Personen verteilt werden können (4-Augen-Prinzip bei großen Rechenzentren).
- Die Administrationsebene ist von der Revisionsebene zu trennen. Der Systemverwalter sollte sich nicht selbst kontrollieren müssen.

Objektintegrität

- Alle sicherheitsrelevanten Objekte (Programme, Prozeduren, Daten) sind durch geeignete manipulationssichere Verfahren so zu versiegeln, daß unautorisierte Veränderungsversuche rechtzeitig, d.h. vor der Ausführung oder Verarbeitung erkannt werden können (Virenschutz).
- Für die Kommunikation sind dem Anwender geeignete Informationssicherungsverfahren (Verschlüsselung, elektronische Unterschrift zum Nachweis der Authentität einer Nachricht) zur Verfügung zu stellen.

Aktive Schutzmechanismen

- Werden Sicherheitsverletzungen als solche erkennt, sind geeignete Gegenmaßnahmen zu ergreifen, die einen Eindringling in seinem Wirkungskreis entweder durch Sperren von Ressourcen oder durch sogenannte Timeout-Routinen (Zeitsperren, Abbruch) beschränken.
- Durch sogenannte Fehlertoleranztechniken (das System erkennt Fehler und stellt den fehlerfreien Zustand selbst wieder her) erreicht man eine Steigerung der Zuverlässigkeit des DV-Systems. Schließlich sind Benutzerdienste zu entwickeln, die umfassender, bedienerfreundlicher und fehlertoleranter sind als die bisherigen.

Revisions- und Dokumentationsebene

- Es muß erkennbar sein, wer wann mit welchen Mitteln auf welche Objekte zugegriffen hat (Protokollierung). Die Protokollierung muß flexibel, d.h. benutzer-, verfahrens- und dateibezogen aktivierbar sein. Auch Fehl- und Mißbrauchsversuche sind aufzuzeichnen.
- Für die Auswertung der Logdateien sind geeignete Programme zur Verfügung zu stellen (Audit-Programme).
- Es muß revisionfähig erkennbar sein, wer wann welche Benutzerrechte besessen hat (Historienverwaltung).
- Es muß manipulationssicher feststellbar sein, wann ein Programm kompiliert und gebunden wurde sowie in welchem Versionsstand es sich gerade befindet. Außerdem muß nachgewiesen werden können, wann welche Programmversion im Einsatz war (Verbindung zu Dokumentation).
- Die Dokumentation sollte in bestimmten Einzelfällen folgende Komponenten umfassen:
  - Beschreibung der Hardwarekomponenten einschließlich der
  - Aufzählung der Datenfernverarbeitungseinrichtungen (Konfiguration Management)
  - Angaben über die Systemgenerierung (Security Level)
  - Zusammenstellung aller Benutzer einschließlich ihrer Rechte (User Management)
  - Liste aller ablauffähigen Programme (Job Management)
  - Querverweislisten über alle Objekte, auf die ein Benutzer Zugriff hat, über alle Prozeduren oder Jobs, die ein bestimmtes Programm aufrufen, und über alle Dateien, die ein bestimmtes Programm verwenden.
  - Auflistung aller Dateien und Datenbanken sowie der Zugriffsberechtigten, wobei beim Zugriff zwischen Lesen, Ändern, Löschen und Ausführen zu unterscheiden ist (Datenmanagement).
- Die Dokumentation ist durch geeignete DV-Verfahren zu unterstützen (Data-Dictionary).
- Der termingerechte Ablauf der Batch-Programme ist über ein Job-Planungssystem zu überwachen. Das Berichtsprogramm muß dazu in der Lage sein, Sollisten und Ausführungsprotokolle mit Angabe der Abweichungen des Ist vom Soll zu erstellen.

Diese Forderungen werden in der Praxis meist noch nicht erfüllt. Durch die Einführung der IT-Sicherheitskriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik wurde jedoch ein großer Schritt in Richtung sichere IT-Systeme geleistet. Die Hersteller sind guten Willens und bieten bereits eine Reihe von Sicherheitskomponenten an, von denen die Anwender insbesondere dann, wenn sensible Daten verarbeitet werden, Gebrauch machen sollten.

22.1.2 Sicherheitsanforderungen bei der Vernetzung von Personal Computern

Die gestiegenen Anforderungen und die technischen Möglichkeiten führen dazu, daß Personal Computer (PC) immer häufiger in einem PC-Netz (Local-Area-Network, LAN) betrieben werden. Wesentliche Anreize sind die Nutzung eines gemeinsamen Daten- und Programmbestandes, der nach seiner Fortschreibung allen Nutzern in einer einheitlichen Version zur Verfügung steht, sowie eine gemeinsame Nutzung von Geräten, wie Druckern oder Festplattenspeichern. Die zentrale Speicherung der Daten und Programme auf dem sog. Server-PC reduziert obendrein die Kosten für den Festplattenspeicher. Im Netz gestaltet sich der Austausch von Daten und Nachrichten einfacher, da das Netzwerkbetriebssystem das Gesamtsystem steuert.

Um das Risiko von Datenmanipulationen zu reduzieren, werden auch diskettenlose PC, sog. Diskless-PC, eingesetzt. Der PC-Nutzer erhält zwar über das Netz Zugriff auf die zentral vorgehaltenen Ressourcen, wie Programme und Daten, kann selbst jedoch weder Daten einlesen noch auf externe Speichermedien, etwa auf eine Diskette, ausgeben.

Die Datensicherheit von Personal Computern in Netzwerken wird von unterschiedlichen Netztopologien und -konfigurationen geprägt. Server-Konzepte bieten neben der Möglichkeit einer zentralen Daten- oder Programmhaltung auch den Vorteil einer zentralen Datensicherung. Darüber hinaus können Benutzerrechte zentral vergeben und verwaltet werden. Die unterschiedlichsten Ressourcen stehen den einzelnen Anwendern nur soweit zur Verfügung, als es zur Aufgabenerfüllung notwendig ist.

Die Installation eines Netzwerkes erfordert einigen Aufwand und ist nicht vergleichbar mit der Einrichtung eines Anwendersystems. Oft sollen in einem Netzwerk auch die unterschiedlichsten DV-Geräte eingebunden werden. Zu beachten ist ferner, daß nicht jedes Netzwerk für sicherheitsrelevante Anwendungen geeignet ist.

Bei der **Einrichtung eines PC-Netzes** sind deshalb folgende Gesichtspunkte zu beachten:

- Aufwand für die Installation und Verwaltung des Netzwerkbetriebssystems
- Einhaltung der Zugriffs- und Verarbeitungssicherheit (Zugriffsschutzverwaltung)
- Erkennen eines Anschlußversuchs eines nicht zugelassenen Personal Computers oder sonstigen Endgerätes
- Aufwand für die Dokumentation des Netzwerkes und die Benutzerrechte (Konfiguration- und User-Management)

- Unterstützung des Recordlockings (Verhinderung, daß sich Benutzer beim gleichzeitigen Zugriff auf Daten gegenseitig blockieren)
- Existenz revisionsfähiger Ablaufdaten
- Maßnahmen zur Erhöhung der Netzwerksicherheit nach Ausfall einer Hardwarekomponente
- Regelung der Ressourcenzugriffssteuerung
- Verschlüsselung der Daten bei der Kommunikation im Netz

Wegen der Bedeutung für die Funktionsfähigkeit des Netzes ist die Vermittlungszentrale (Server) besonders zu schützen. Gleiches gilt auch für Netzwerkverteilerschränke als Übergabestationen (Gebäude- oder Etagenverteiler).

In weit verzweigten Netzen, die besonderen Anforderungen an die Ausfallsicherheit genügen müssen, sind folgende Sicherheitsmaßnahmen bereits in der Planungsphase zu berücksichtigen:

- Fernüberwachung
- Ferndiagnose
- Fernsteuerung
- Vorhalten redundanter Verbindungen, um dem Ausfall einer Leitung wirksam begegnen zu können
- LAN-Hauptstränge, sog. Backbones, möglichst doppelt ausgelegt
- automatischer Wiederaufbau der Leitungsverbindungen nach einem Netzzusammenbruch (automatisches Rerouting)

Die zentralen Einheiten, wie Netzknotensteuerung und Stromversorgung, sollten redundant ausgelegt sein und bei Ausfall eines Gerätes eine vollautomatische Umschaltung auf das Ersatzgerät ermöglichen. Von besonderer Bedeutung für die Netzwerkadministration bei festgestellten Fehlern oder bei der Wartung ist, daß eine aktuelle, möglichst DV-gestützte Netzwerkdokumentation bereitgestellt wird.

Da Stromausfall und Spannungsschwankungen zu den häufigsten Störquellen zählen, müssen die Netzknoten durch eine unterbrechungsfreie Stromversorgung, redundante Netzteile und Spannungsstabilisatoren geschützt werden. Daß bei bestimmten Übertragungsmedien, etwa bei Kupferkabeln, besondere Schutzmaßnahmen, wie Blitzschutz, Erdung und Potentialausgleich vorzusehen sind, sollte berücksichtigt werden.

Für die Steuerung und die Sicherheit des Netzwerkes ist ein geeignetes **Netzwerkbetriebssystem** erforderlich. Wesentliche Sicherheitsfunktionen eines solchen Netzwerkbetriebssystems sind u.a.:

- Zugangs- und Zugriffsverwaltung
  - Transparenter Zugriff auf verfügbare Ressourcen
  - Überwachung des Zugriffs durch geeignete Sicherheitsmechanismen
  - Verwaltung der Serverfunktionen
  - Schutz gegen Anschluß unbekannter Geräte
- Benutzerverwaltung
- Ressourcen Management
- automatische Konfigurierung bei Vorgabe der Anzahl der Knoten
- Nachrichtensteuerung
- benutzerspezifische Menüsteuerung
- Verwaltung der Elektronic Mail
- Aufzeichnung von signifikanten Ablaufdaten für Kontroll- und Revisionszwecke

Schließlich ist zur Gewährleistung der Datensicherheit beim PC-Einsatz im Netz ein verantwortlicher Netzadministrator zu bestimmen, dessen Rechte eindeutig festgelegt sein müssen. Alle die Sicherheit betreffenden Festlegungen und Vereinbarungen sind zu dokumentieren und bei Veränderungen revisionsfähig zu halten. Positiv zu werten ist es, wenn das Netzwerkbetriebssystem selbständig eine revisionsfähige Dokumentation über alle angeschlossenen und verfügbaren Ressourcen führt. Besonders wichtig ist aber, daß der Netzwerkadministrator unverzüglich informiert wird, wenn der Versuch des Anschlusses eines fremden Gerätes gemeldet wird, auch dann wenn dieses Gerät vom Netzwerkcontroller bereits abgewiesen wurde.

Das Netzwerkbetriebssystem ist im allgemeinen auf dem Netzwerkserver gespeichert. Zum **Schutz des Netzwerkservers** sind folgende Maßnahmen zu empfehlen:

- Der Netzwerkserver ist in einem besonders geschützten Bereich und unter Beachtung geeigneter Zugangs- und Zugriffsschutzmaßnahmen einzurichten.
- Dem Datenverlust durch Stromausfall kann man am besten mit einer unterbrechungsfreien Stromversorgung vorbeugen, mit der solche Server standardmäßig ausgestattet sein sollten.
- Eine manipulationssichere Soft- und Hardware steuert den Zugriff auf die Server-Dienste und Server-Files.

Zu bedenken ist schließlich noch das Risiko, daß man durch mechanisches Ausschalten des Servers einen ungehinderten Zugang zu allen LAN-Ressourcen an diesem Server erhalten kann. Deshalb empfiehlt es sich, den Netzwerkserver zusätzlich durch folgende Maßnahmen zu sichern:

- Mechanische Verriegelung des Gehäuses zur Verhinderung des Zugangs zum Geräteinneren
- Schutz des Rechners vor mißbräuchlicher Inbetriebnahme durch ein elektronisches Sicherheitsschloß
- Verschlüsselung der Daten auf dem Massenspeicher

22.1.3 Einsatz der Chipkarte

Eine weitere Möglichkeit, den Bearbeitungs- und Zugriffsschutz an Bildschirmarbeitsplätzen zu erhöhen, bildet neuerdings der Einsatz von Magnet- oder Chipkarten. Die Magnet- oder Chipkarte erfordert allerdings eine zusätzliche Leseeinrichtung. Bei der Identifizierung des Benutzers wird geprüft, ob die Person, die diese Ausweiskarte benutzt, auch tatsächlich zur Benutzung berechtigt ist. Diese Prüfung erfolgt über die persönliche Identifikationsnummer (PIN), die der Benutzer entweder an der Tastatur oder direkt am Chipkartenlesegerät eintippt. Mit der Chipkarte können auch Verschlüsselungsroutinen gekoppelt sein. Bei Einsatz der Chipkarte kann die Sicherheit schließlich noch erhöht werden, daß die Identifikationsmerkmale nicht über die Leitung zum Zentralrechner übertragen, sondern vor Ort im Chipkartenlesegerät und innerhalb der Chipkarte geprüft werden.

Da der Einsatz der Chipkarte einen höheren finanziellen Aufwand bedeutet, ist zu überlegen, welche Arbeitsplätze mit solchen zusätzlichen Sicherheitsmaßnahmen ausgerüstet werden sollen. Dabei bieten sich in erster Linie solche Arbeitsplätze an, von denen systemrelevante Aktionen ausgeübt werden können, etwa die Systemverwaltung, die Benutzerverwaltung, die Datenübertragung mittels Filetransfers oder ähnlich privilegierte Funktionen.

Für UNIX-Systeme werden heute Chipkarten-Systeme angeboten, die ohne Lesegerät auskommen und deshalb auch weniger Kosten verursachen. Die Arbeitsweise eines solchen Systems basiert auf einem Programm im Rechner, das die Chipkarten mit den entsprechenden Passcodes verwaltet und generiert. Jeder Passcode hat für eine bestimmte Chipkarte lediglich 60 Sekunden Gültigkeit. Will ein Benutzer mit dem DV-System in Verbindung treten, aktiviert er die Chipkarte mit seiner gleichbleibenden Geheimnummer und erhält dann den zu dieser Zeit gültigen Passcode, der eingetippt und vom DV-System geprüft wird. Chipkarten und DV-System müssen deshalb gleich getaktet sein. Die Sicherheit des Verfahrens wird dadurch erhöht, daß die Gültigkeit des Passcodes begrenzt ist, keine Paßworte auf Leitungen übertragen werden und die Chipkarte auf ungültige Geheimnummerneingabe durch entsprechende Maßnahmen (Sperrung) reagiert.

Da die Chipkarte erst seit kurzem verfügbar ist, liegen noch keine Erfahrungen über die Akzeptanz in der Praxis vor.

22.2 Prüfungstätigkeit

22.2.1 Kontrolle und Beratung

Die Einhaltung von technisch-organisatorischen Maßnahmen zur Datensicherheit habe ich im Berichtszeitraum bei folgenden öffentlichen Stellen kontrolliert:

- Betriebskrankenkasse der Stadt Augsburg
- Kreiskrankenhaus Bamberg
- Landesversicherungsanstalt Schwaben, Augsburg
- Landratsamt Fürth
- Landratsamt Wunsiedel
- Landratsamt Würzburg
- Polizeiinspektion Rosenheim
- Rechenzentrum des Polizeipräsidiums Mittelfranken
- Innungskrankenkasse Regensburg
- Landwirtschaftliche Alters- und Krankenkasse Oberbayern
- Allgemeine Ortskrankenkasse Aschaffenburg
- Amt für Landwirtschaft Weilheim
- Realsteuerstelle Regensburg
- Vermessungsamt Erlangen
- maschinelle Datenverarbeitung bei einer Hauptschule
- Datenverarbeitung der Finanzämter Ingolstadt und Rosenheim

Ferner habe ich bei folgenden DV-Verfahren die Sicherheitsmaßnahmen überprüft:

- Dialogverfahren für die Bezügeabrechnung bei der Bezirksfinanzdirektion München, Bezügestelle 1
- Krankenhauskommunikationssystem bei der Universität Würzburg

Wie im Vorjahr habe ich auch 1991 die Datenträgerentsorgung bei insgesamt 24 speichernden Stellen kontrolliert. Schwerpunkt bei dieser Kontrolltätigkeit ist die datenschutzgerechte Entsorgung von Papier und sonstigen Unterlagen mit personenbezogenen Inhalten.

Die Beratungstätigkeit meiner Dienststelle in Fragen der Datensicherheit beim Um- und Neubau von Dienstgebäuden und Rechenzentren der bayerischen öffentlichen Verwaltung nahm im Berichtszeitraum wiederum einen breiten Raum ein. Insgesamt haben sich etwa 20 Dienststellen an mich gewandt und Empfehlungen und Vorschläge zur Gebäudesicherheit und zur Sicherheit im DV-Bereich eingeholt. Bei dieser Vorgehensweise lassen sich erhebliche finanzielle Mittel einsparen, die dann aufgewendet werden müßten, wenn Einrichtungen zum Datenschutz und zur Datensicherheit erst nach Abschluß der Baumaßnahmen installiert werden.

Die Nachfrage nach Orientierungshilfen für Datensicherheitsmaßnahmen beim Einsatz von Anlagen des Typs Hewlett Packard 3000, Digital-Kienzle 9000, Siemens MX 300/MX 500 und IBM AS/400 war im Berichtszeitraum wiederum sehr lebhaft.

Das Thema „PC-Sicherheit" behandelt eine Veröffentlichung in der Zeitschrift für Kommunikations- und EDV-Sicherheit KES, erschienen im Januar-Heft

91/1 beim Secumedia-Verlag, 6507 Ingelheim, unter der ISSN-Nr. 0177-4565. Die Zusammenstellung, die von Mitarbeitern meiner Dienststelle verfaßt worden ist, befaßt sich mit Grundlagen der PC-Sicherheit, der Organisation, mit Installationsanforderungen, mit Regeln gegen Datenverlust, mit Maßnahmen gegen den Datenmißbrauch, insbesondere beim Standalone-Betrieb und gegen Viren und ihre Bekämpfung, mit der Beschreibung der Vorteile für Serverkonzepte und mit Kontrollmaßnahmen zum Datenschutz. Außerdem werden Hinweise angeboten für die Rettung von Daten und Programmen im Not- und Katastrophenfall, um materielle Schäden möglichst gering zu halten. Die Veröffentlichung kann im begrenzten Umfang noch bei meiner Geschäftsstelle oder über den Secumedia-Verlag bezogen werden. Ausführlich wurde dieses Thema im Fachbuch „PC-Sicherheit im Unternehmen" (Autoren: Abel, Schmölz; Verlag C.H. Beck, München; 1991) behandelt.

22.2.2 Ergebnisse der Kontrolltätigkeit

Als Ergebnis meiner Kontrolltätigkeit im Berichtszeitraum ist festzuhalten, daß in der öffentlichen Verwaltung die Bereitschaft, Maßnahmen zum Datenschutz und zur Datensicherheit zu treffen, weiter zugenommen hat. Allerdings werde ich auch häufig auf die angespannte Haushaltslage hingewiesen, wodurch sich die Realisierung der erforderlichen Maßnahmen zum Datenschutz und zur Datensicherheit verzögert.

Anhand von allgemein interessierenden Beispielen sollen einige Mängel und Maßnahmen zu deren Behebung aufgezeigt werden.

Notfallkonzept

Die Behörden investieren immer mehr Geld in den Ausbau ihrer elektronischen Datenverarbeitung, vergessen aber oft, Vorsorgemaßnahme zu treffen und ein Notfallkonzept zu erstellen, obwohl die Aufrechterhaltung des Dienstbetriebs heute zunehmend von der ununterbrochenen Funktionsfähigkeit der DV-Anlagen abhängt.

Bei der Erstellung eines Notfallkonzepts sind alle möglichen Beeinträchtigungen der Hardware (z.B. Ausfall des Rechners, Ausfall einer Platte oder des Netzwerkes) und der Software (z.B. fehlerhafte Systemsoftware nach einer Betriebssystemumstellung) zu bedenken und entsprechende Sicherheitsmaßnahmen vorzusehen. Das Notfallkonzept sollte zumindest einmal jährlich überdacht und den Gegebenheiten angepaßt werden. Um festzustellen, ob die geplanten Maßnahmen in die Praxis umgesetzt werden können, sind sie in regelmäßigen Abständen zu testen. Dies dient zugleich der Schulung des Personals für den Notfall. Beim Test aufgetretene Fehler und Unstimmigkeiten sind im Notfallkonzept umgehend zu beheben.

Auswertung von Log-Dateien

Viele Betriebssysteme bieten heutzutage die Möglichkeit, alle Zugriffe und Tätigkeiten auf dem Rechner zu **protokollieren** und **auszuwerten**. Bei meinen Prüfungen mußte ich jedoch feststellen, daß diese Möglichkeit der Kontrolle der Ablaufdaten zumeist nicht genutzt wird. Ich möchte daher noch einmal darauf hinweisen, daß zum Nachweis der Ordnungsmäßigkeit der Datenverarbeitung die vom Betriebssystem — oder einer Anwendung — geschriebenen Log-Protokolle regelmäßig auf Unregelmäßigkeiten im System oder in den Anwendungen zu überprüfen sind. Die Überprüfung ist zu dokumentieren.

Wegen der zunehmenden Vernetzung der Rechner ist dabei besonderes Augenmerk auf die Verletzung bzw. den Versuch einer Umgehung der Zugriffsschutzmaßnahmen zu legen.

Deaktivierung von Bildschirmen

Anwender von zentralen und teildezentralen Verfahren der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) müssen wegen der Datenübertragung zum und vom Zentralrechner der AKDB die dezentralen Rechner rund um die Uhr betriebsbereit halten. Wenngleich auch die einzelnen Verfahren durch die zwingende Eingabe von Benutzerkennungen und persönlichen Paßworten geschützt sind, ist eine unbefugte Benutzung der dezentralen Systeme nicht auszuschließen. Aus diesem Grunde sind die Bildschirmarbeitsplätze nach Dienstende durch geeignete Verfahren zu deaktivieren, so daß eine mißbräuchliche Verwendung ausgeschlossen ist.

Verwendung von Laptop-Geräten

Bei verschiedenen Dienststellen habe ich festgestellt, daß diese ihren Bediensteten für die Datenerfassung vor Ort tragbare Personal Computer, sogenannte Laptops, zur Verfügung stellen. Es ist dabei nicht auszuschließen, daß diese Geräte auch in den häuslichen Bereich des Bediensteten gelangen können. Werden auf diesen Laptop-Geräten personenbezogene Daten verarbeitet, so muß durch den Einsatz entsprechender Software die unbefugte Kenntnisnahme der dienstlichen Daten verhindert werden. Eine Verschlüsselung der gespeicherten Daten verhindert jede mißbräuchliche Kenntnisnahme gespeicherter Daten. Außerdem muß in einer Dienstanweisung festgehalten werden, wie der PC, sobald er den dienstlichen Bereich verlassen hat, gegen eine Fremdnutzung oder Diebstahl zu sichern ist. In einem Anwendungsfall mußte ich feststellen, daß die Datenbereiche auf der Festplatte nicht gelöscht werden, wenn der Laptop einem anderen Bediensteten mit anderen Aufgaben zur Nutzung übergeben wird. Außerdem war über ein solches Gerät ein unkontrollierter Zugriff auf am Großrechner gespeicherte Daten möglich (Akustikkoppler, Wählleitung). Durch geeignete Maßnahmen

(Beschränkung des Anwendungsspektrums auf die erforderlichen Aufgaben) konnte diese Schwachstelle beseitigt werden.

Persönlichkeitsschutz an Behördenschaltern

Aufgrund des gestiegenen Datenschutzbewußtseins der Bürger erreichen mich immer wieder Beschwerden aus der Öffentlichkeit, die sich über den mangelnden Persönlichkeitsschutz an **Behördenschaltern** beklagen. Gerade Dienststellen, bei denen viel Publikumsverkehr abgewickelt wird und sensible Informationen ausgetauscht werden, sollten geeignete Maßnahmen ergreifen, um das Recht des Bürgers auf den Schutz seiner Persönlichkeit zu gewährleisten. Ist es aus räumlichen Gründen unabdingbar, daß sich zwei oder mehr Sachbearbeiter ein Zimmer teilen, so muß zumindest ein **gesonderter Raum für Einzelgespräche** bereitstehen. Auf diese Möglichkeit einer diskreten Sachbehandlung muß durch entsprechende Anschläge hingewiesen werden. Außerdem sollten die zuständigen Sachbearbeiter in einer schriftlichen Dienstanweisung verpflichtet werden, die Bürger bereits bei der ersten Kontaktaufnahme auf die Möglichkeit der Einzelberatung bei sensiblen Themen hinzuweisen.

Entsorgung von Datenträgern

Im Berichtszeitraum wurden wieder 24 Behörden speziell hinsichtlich der datenschutzgerechten Entsorgung von Datenträgern mit personenbezogenen Inhalt überprüft. Dabei mußte ich wiederholt feststellen, daß sich manche Dienststellen vor allem bei der Entsorgung von Papierunterlagen mit personenbezogenen Daten doch recht fahrlässig verhalten. Zum Teil existieren nicht einmal schriftliche Dienstanweisungen, in denen die Mitarbeiter auf die datenschutzgerechte Vernichtung dieser Unterlagen verpflichtet werden. Wie in meinem 12. Tätigkeitsbericht möchte ich noch einmal darauf hinweisen, daß durch die Beschaffung von Reißwölfen, die der DIN 32757 entsprechen müssen, das Problem am einfachsten zu lösen ist. Diese Aktenvernichter sollten zweckmäßigerweise neben den vorhandenen Kopiergeräten stehen, so daß eventuelle Fehlablichtungen mit personenbezogenen Daten dort entsorgt werden können.

In letzter Zeit nehmen die Hersteller von **Carbonfarbbändern** die Kassetten mit den beschriebenen Carbonfarbbändern zurück, um aus Gründen der Materialersparnis die Gehäuse mit neuen Carbonfarbbändern zu bestücken. In derartigen Fällen müssen mit dem Hersteller der Carbonfarbbänder vertragliche Regelungen getroffen werden, die eine Verwertung der beschriebenen Bänder durch den Hersteller oder durch Dritte ausschließen.

Bisher sind Carbonfarbbänder häufig durch Verbrennen entsorgt worden. Aus Umweltschutzgründen ist eine solche Entsorgung nicht mehr vertretbar. Eine datenschutzgerechte Lösung wäre, die Kassetten mit den Carbonfarbbändern in einem Schreddergerät zu zerkleinern. Diese Geräte, die immerhin ca. DM 4000,— kosten, werden von kleineren Verwaltungseinheiten aus Kostengründen aber selten beschafft. Ich empfehle daher, daß vorgesetzte Dienststellen für ihren nachgeordneten Bereich ein Schreddergerät beschaffen und es den nachgeordneten Dienststellen zum Gebrauch zur Verfügung stellen.

Meldungen zum Datenschutzregister

Die Meldungen der Dienststellen zum Datenschutzregister sind häufig über zehn Jahre alt. Mittlerweile haben sich solche DV-Verfahren in wesentlichen Teilen geändert oder sind durch modernere DV-Verfahren abgelöst worden. Bei meinen Kontrollen habe ich immer wieder feststellen müssen, daß die Meldungen zum Datenschutzregister nicht mehr dem DV-Verfahrenseinsatz zum Prüfungszeitpunkt entsprechen. Es ist deshalb erforderlich, daß die Dienststellen den Stand und die Aktualität ihrer abgegebenen Meldungen zum Datenschutzregister von Zeit zu Zeit überprüfen und, wenn notwendig, neue Datenschutzregistermeldungen abgeben.

22.2.3 Datenverarbeitung bei der Steuerverwaltung

Die Steuerverwaltung bedient sich der automatischen Datenverarbeitung schon seit vielen Jahren. Großrechneranlagen stehen bei den Zentralfinanzämtern der Oberfinanzdirektionen München und Nürnberg. Die dezentralen DV-Komponenten (Vorrechner, Terminals) in den Finanzämtern sind über Standleitungen (HfD-Leitungen) an die Rechner der beiden Zentralfinanzämter angeschlossen. Die in den Finanzämtern installierten Vorrechner dienen als Datensammelrechner. Zu bestimmten Zeiten ruft der jeweilige Zentralrechner die Änderungsdaten zur Verarbeitung ab. Zur Einsparung von Leitungskosten sind manche Vorrechner noch mit einem Knotenrechner verbunden. Über eigene Programme wird sichergestellt, daß jedes Finanzamt nur auf die eigenen Daten zugreifen kann.

Wegen der hohen Sensibilität der gespeicherten steuerlichen Daten und zur Gewährleistung des Steuergeheimnisses hat die Steuerverwaltung erfreulicherweise zwischenzeitlich erhebliche Anstrengungen unternommen, den Zutritt zu den DV-Bereichen und den Zugriff auf die gespeicherten Daten nur den dafür zuständigen Bediensteten zu ermöglichen. Die Zugangssicherungen bestehen aus modernen elektronischen Sicherheitseinrichtungen, die auflaufende Alarme selbsttätig an ständig besetzte und kompetente Meldestellen abgeben. Der interne Zugriffsschutz auf gespeicherte Steuerdaten wird unter Ausnutzung der Sicherheitskomponenten der Betriebssysteme, der systemnahen Basissoftware und der Anwendungssysteme gewährleistet.

Die dezentrale Datenverarbeitung auf der Basis von Personal Computern ist in der bayerischen Steuerverwaltung erst im Aufbau begriffen. Gegenwärtig befindet sich bei den Betriebsprüfungsstellen ein selbst entwickeltes, die Prüfungsvorbereitungen und die Auswertung der Prüfungsergebnisse unterstützendes DV-Verfahren im Piloteinsatz. Steht dieses Verfahren einmal allen Betriebsprüfungsstellen zur Verfügung, ist die derzeit noch eingeschränkt erlaubte Verwendung privater Hard- und Software zu dienstlichen Zwecken nicht mehr erforderlich.

Zusätzlichen Zugriffsschutz vor unberechtigtem Datenabruf innerhalb der Steuerverwaltung brächte die **Steuerdatenabrufverordnung**, deren Erlaß durch den Bundesfinanzminister aber nach wie vor noch aussteht. Bei der Einrichtung eines Datenabrufverfahrens für bestimmte abrufberechtigte Amtsträger oder Dienststellen werden künftig selbsttätig die identifizierenden Daten des Abrufenden und des verwendeten Endgeräts sowie der Abrufgrund **protokolliert**. Dadurch ist kontrollierbar, ob der Datenabruf berechtigterweise erfolgt ist.

22.3 Technische Einzelprobleme

22.3.1 Datensicherheit bei Teletex

Die Automatisierung der Büroarbeit schreitet weiter voran. Im 12. Tätigkeitsbericht wurde auf Seite 64 die Datensicherheit bei Telefax behandelt. Eine weitere, immer häufiger anzutreffende Form der Kommunikation stellt der Telekom-Dienst Teletex dar. Teletex, auch Bürofernschreiben genannt, wird als die elektronische Form des Fernschreibens bezeichnet und ist eine nachrichtentechnische Textkommunikation mit einem genormten Zeichenvorrat. Technisch wird Teletex in einer eigenen Benutzerklasse innerhalb des Datex-L-Netzes abgewickelt. Eine Zwischenspeicherung eines Teletex-Briefes in den Fernmeldevermittlungsstellen findet nicht statt, so daß ein mißbräuchlicher Zugriff weitgehend ausgeschlossen ist. Es handelt sich hier lediglich um ein Durchreichen, so daß Telekom nur Vermittlungs- und Transportdienste leistet.

Geht eine Nachricht an mehrere Adressaten, so erfolgt die Übertragung sequentiell aus dem Sendespeicher des Absenders, wobei der Empfänger als Hinweis für einen eingegangenen Text ein optisches Signal erhält. Als Verständigungsprotokoll dient eine Kommunikationsdatenzeile. In diesem Bereich werden die Kennung der gerufenen und der rufenden Station, das Datum und die Sendezeit sowie die Dokumenten- und Seitennummer als Referenzinformation des Absender zur Nachricht eingestellt.

Ein Abhören des Nachrichtenaustausches auf den Übertragungswegen ist technisch möglich, soweit die Informationen nicht verschlüsselt werden. Ein gezieltes Durchgreifen auf bestimmte Informationsflüsse gilt jedoch als unwahrscheinlich. Ein mißbräuchlicher Zugriff auf den Sende- oder Empfangsspeicher erfordert die Simulation einer Fernmeldevermittlungsstelle und die genaue Kenntnis der Kommunikationsprotokolle sowie die Kenntnis über die speziellen Hilfsmechanismen wie Paßwort, Systemkenndaten. Die Wahrscheinlichkeit, daß bei einer Teletex-Verbindung Daten an Dritte gelangen, ist deshalb äußerst gering.

22.3.2 Betrieb von Telekommunikationsanlagen

Die Zahl der digitalen Telekommunikationsanlagen wächst ständig. Im 12. Tätigkeitsbericht habe ich auf Seite 63 Hinweise für den Betrieb von Telekommunikationsanlagen gegeben. Außerdem habe ich eine Orientierungshilfe für den datenschutzgerechten Betrieb digitaler Telekommunikatinsanlagen entwikkelt, die speziell auf die bayerischen Belange abgestimmt ist. Interessenten erhalten diese Orientierungshilfe zum Betrieb digitaler Telekommunikationsanlagen bei meiner Geschäftsstelle.

22.3.3 Version 10 von BS2000

In den Großrechenzentren der bayerischen Behörden werden eine Reihe von Rechnern der Siemens-Nixdorf Computersysteme AG (SNI) mit dem Betriebssystem BS2000 eingesetzt, so daß es angezeigt ist, hier auf die neuesten sicherheitstechnischen Entwicklungen hinzuweisen. Mit der Version 10 des BS2000 bietet SNI das Sicherheitskontrollsystem SECOS (Security Control System) an. SECOS enthält folgende Komponenten: das Rechtezuordnungssystem SRPM (System Resources and Privileges Management), das Zugriffsschutzsystem FACS (Full Access Control System) und das Protokollsystem SAT (Security Audit Trail). Mit SECOS hat die SNI die Einstufung des BS2000 in die Sicherheitsstufe F2/Q3 des nationalen IT-Kriterienkatalogs erreicht.

Mit SRPM besteht die Möglichkeit, die Rechte der Systemverwalterkennung TSOS auf mehrere Personen zu verteilen. Alle protokollwürdigen Daten über Systemaktivitäten werden von SAT in sogenannten Collection-Files gesammelt. Diese Dateien sind mit dem Dienstprogramm SATUT auswertbar. SAT überwacht derzeit 26 Ereignistypen (wie Programmstart, Dateieröffnung etc.) und über 100 objektspezifische Ereignisarten. Je nach Schalterstellung wird ein Ereignis immer, nicht bzw. im Erfolgs- oder Mißerfolgsfall protokolliert. Es gibt aber auch Ereignisse, deren zwingende Protokollierung vom Anwender aus Sicherheitsgründen nicht beeinflußt werden kann. Protokollierung und Auswertung können bei SAT von zwei autorisierten Benutzern verwaltet werden, wodurch das 4-Augen-Prinzip gewährleistet wird. Bei der Definition der Standardeinstellungen konnten meine Vorstellungen vom Hersteller berücksichtigt werden.

Bei der Verarbeitung von personenbezogenen Daten rate ich allen BS2000-Anwendern, die Version 10 des BS2000 zusammen mit SECOS so bald wie möglich zu installieren und von den sicherheitsrelevanten Komponenten unbedingt Gebrauch zu machen.

22.3.4 Überspannungsschutz und unterbrechungsfreie Stromversorgung

Mit zunehmender Vernetzung gewinnt der Überspannungsschutz und die unterbrechungsfreie Stromversorgung an Bedeutung. Untersuchungen von Versicherungsgesellschaften haben nämlich ergeben, daß über 50 % der Verarbeitungsfehler auf **Störungen der Stromversorgung** zurückzuführen sind. Im Gegensatz zur Elektrik muß in der Eletronik die elektrische Energie frei von Kurzunterbrechungen, Störwellen, Spannungs- und Frequenzschwankungen sein. Die Folgekosten eines Netzausfalles können beachtlich sein, wenn Daten nicht ordnungsgemäß und rechtzeitig gesichert wurden. Ein Personal Computer ist bereits gegen geringe Netzschwankungen anfällig, was zum Verlust von Daten zumindest bei den DOS-Systemen, die über keinen Netzpuffer verfügen, führen kann. Hingegen führen UNIX-Systeme in bestimmten Zeitintervallen eine Sicherung der Daten im Arbeitsspeicher auf die Platte durch.

Schaltüberspannungen durch Zu- und Abschalten von großen Stromverbrauchern, manchmal sogar von Leuchtstoffröhren verursacht, sowie durch Blitzschlag und andere Störungen sind die häufigste Ursache für einen solchen Ausfall. Überspannungen können aber auch durch elektrische Induktion entstehen. So haben die indirekten Blitzschlagschäden in den letzten Jahren zugenommen. Ein Grund für den Anstieg dieser Störungen wird vor allem in der zunehmenden PC-Vernetzung gesehen, da die Datenleitungen die Sekundärimpulse verteilen und sich sogar gegenseitig beeinflussen können. Die sinkende Qualität der Verbrauchernetze als Folge der Zu- bzw. Abschaltung großer Lasten ist eine weitere Störquelle.

Diesem Risiko kann der Anwender durch Einsatz unterschiedlicher Geräte mit unterbrechungsfreier Stromversorgung (USV) und zum Überspannungsschutz begegnen. USV-Geräte stellen die Stromversorgung über einen bestimmten Zeitraum sicher, so daß genügend Zeit für eine Datensicherung und ein kontrolliertes Beenden der Verarbeitung verbleibt. Beim Überspannungsschutz wird der Impuls vom DV-Gerät ferngehalten. Unterschieden werden sogenannte Stand-by-Systeme und Online-Geräte, die jedoch wesentlich teuer sind als Stand-by-Geräte. Die Leistung reicht von 300 bis maximal 2000 Watt, die Überbrückungszeit bei Vollast liegt im Bereich von einer Minute bis zu 60 Minuten.

Spannungsschwankungen können durch den Einsatz sogenannter Störschutztransformatoren, Störschutzfilter und Störschutzadapter beseitigt werden. Schließlich ist es auch möglich, Netzverteilerkästen oder Steckdosenleisten zu installieren, die die daran angeschlossenen Geräte mit einer gleichbleibenden Netzspannung versorgen und alle Spannungsschwankungen sowie Sekundärspannungen vernichten.

Es gibt eine Reihe von Herstellern, die ein Komplettprogramm an Geräten und Elementen für einen vollständigen Schutz anbieten: Gegen Überspannungen, wie sie durch Blitzschläge verursacht werden, gegen Schaltspannungen, die beim An- bzw. Abschalten von elektrischen Geräten entstehen können, sowie gegen elektrostatische Aufladungen. Als Schutz gegen induzierte Blitzspannungen gibt es Blitzschutzpotentialausgleichsgeräte als sogenannten Grobschutz. Für den Feinschutz werden Überspannungsschutzgeräte angeboten, die direkt am zu schützenden Gerät anzubringen sind.

22.3.5 Datensicherheit beim APC-Einsatz

Ein Beispiel für **ergänzende Sicherheitsmaßnahmen** beim Einsatz von Arbeitsplatzcomputern sind die zusätzlichen Anweisungen des Bayer. Staatsministeriums des Innern. Aufgrund der Prüfungsbemerkungen nach einer technisch-organisatorischen Kontrolle bei einer Polizeiinspektion, die nach dem neuen Konzept mit mehrplatzfähigen Arbeitsplatzcomputern ausgestattet ist, hat das Innenministerium u. a. folgende Maßnahmen zur Verbesserung der Datensicherheit bei den Polizeiinspektionen angeordnet:

- Die Systemverwalter sollen regelmäßig alle Protokolldateien auswerten, um unberechtigte Zugriffsversuche festzustellen.
- Der Anwendungsbetreuer hat Benutzerprofile vorzuhalten, aus denen erkennbar ist, wer wann welche Zugriffsrechte besitzt.
- Zur Vermeidung von Brand- oder Wasserschäden im Rechnerraum sind geeignete Meldeeinrichtungen zu installieren und Vorkehrungen zu treffen, im Schadensfall zunächst selbst eine Schadensbegrenzung zu erreichen, bis Hilfe von außen kommt.
- Sicherungsdatenträger dürfen nicht im Rechnerraum hinterlegt werden, damit im Schadensfall nicht Daten und Rechner zugleich verloren gehen.
- Wo es notwendig ist, ist der Zugang zum Rechnerraum abzusichern. Die Zugangstüre ist mit einer automatischen Schließeinrichtung auszustatten.

Diese Entwicklung begrüße ich sehr. Das Bayerische Staatsministerium des Innern läßt damit erkennen, welchen hohen Stellenwert es der Datensicherheit bei Verarbeitung sensibler personenbezogener Daten beimißt.

Daß die Datensicherheit nicht überall gewährleistet ist, zeigt ein Beispiel einer anderen Behörde.

Trotz einer weiten Verbreitung von Personal Computern wird auf notwendige Sicherheitsmaßnahmen verzichtet, weil noch ungeklärt ist, ob die Rechner im Stand-alone-Betrieb oder vernetzt eingesetzt werden sollen. Für MS-DOS-Rechner gibt es eine Reihe von Sicherheitsprodukten, welche die jeweiligen Sicherheitsbedürfnisse abdecken. Es gibt Hersteller, die je nach Betriebsart aufeinander abgestimmte Produkte anbieten.

Werden sensible Daten auf Stand-alone-Geräten gespeichert, sind diese zu verschlüsseln, damit bei einem Gerätediebstahl keine interpretierbaren Daten in die Hände Unbefugter fallen.

Die Zahl der bekannten **Computerviren** hat sich 1991 auf fast 1000 mindestens verdoppelt. Viele Institutionen bieten bei der Virenbekämpfung ihre Dienste an, etwa Viren rechtzeitig ausfindig zu machen und aus infizierten DV-Systemen zu entfernen. Es gibt eine Reihe von Programmen, die allerdings nur bekannte Virussignaturen erkennen können. In mindestens 95 Prozent aller Fälle reicht das bereits aus, die Anwender bei der Bekämpfung von Computerviren wirksam zu unterstützen, da sehr viele Virusarten relativ selten oder noch nicht genug verbreitet sind. Die meisten Virusschutzprogramme werden aber vierteljährlich ergänzt, so daß auch die zwischenzeitlich neu aufgetauchten Viren erkannt werden.

Viele dieser Maßnahmen werden aber entbehrlich, wenn sich die APC-Benutzer an die vorgegebenen Richtlinien halten und nur solche Software-Produkte einsetzen, die von der zentralen Stelle für die Koordinierung des APC-Einsatzes (Benutzerservice) freigegeben wurden. Die Quellen von Computerviren sind nämlich meinen Erkenntnissen nach in erster Linie Spielprogramme und nicht lizenzierte Kopien von Standardsoftware aus sog. Software-Billigländern.

22.3.6 Abschottung der statistischen Datenverarbeitung

Die Verwendung der Ergebnisse der Volkszählung 87 durch kommunale Statistikstellen wirft auch technisch-organisatorische Fragen auf. Die kommunale Statistik ist zur Erledigung ihrer Aufgaben meist an die gemeindeeigene DV-Anlage angeschlossen. Wegen des Abschottungsgebots sind die im Rechenzentrum zu realisierenden Sicherungsmaßnahmen mit denen eines Mehrzweckrechenzentrums vergleichbar, wo die Benutzer durch technische Maßnahmen gegeneinander abzuschotten sind, so daß keine Querverbindungen möglich sind.

Die großen Kommunen in Bayern mit abgeschotteten Statistikstellen bedienen sich meist noch der zentralen DV-Anlage, die hauptsächlich für die Aufgaben des Verwaltungsvollzugs genützt wird. Für einen solchen Betrieb habe ich folgende Datensicherungsmaßnahmen gefordert:

- Die Programme und Daten der Statistik müssen durch Paßworte gegen unbefugte Verwendung gesichert sein, wobei die Paßwortverwaltung und -änderung der Statistikstelle obliegen muß.
- Der Zugriff auf Daten der Statistikstelle ist auf solche Endgeräte zu beschränken, die sich in der abgeschotteten Statistikstelle befinden.
- Der Leiter der Statistikstelle erhält regelmäßig (etwa einmal wöchentlich) ein Protokoll, aus dem hervorgeht, wer wann auf welche Statistikdaten mit welchem Programm zugegriffen hat.
- Die ausgelagerten externen Datenträger mit Statistikdaten sind in einem eigenen Schrank von den übrigen Datenträgern getrennt aufzubewahren.
- Der Transport von Datenträgern und Auswertungen muß entweder durch Personal der Statistikstelle oder in verschlossenen Behältnissen gegen Nachweis erfolgen.
- Im Rechenzentrum ist eine Dokumentation zu führen, aus der hervorgeht,
  - mit welchen Programmen und Datenbeständen die Statistik stelle arbeitet,
  - wer wann welche Zugriffsrechte auf Statistikdaten besitzt und besessen hat und
  - welche externen Datenträger geschützte Statistikdaten enthalten.

22.3.7 Plausibilitätsprüfungen

Bei der Erstellung von Programmen für neue Anwendungsverfahren stellt sich immer wieder die Frage nach der Art und dem Umfang von Plausibilitätsprüfungen bei der Dateneingabe.

Plausibilitätsprüfungen können entweder formaler oder logischer Art sein. Während der Einsatz formaler Plausibilitsprüfungen, z.B. Überprüfung des Feldinhaltes auf alphanumerische Zeichen, auch heutzutage erforderlich ist, müssen der Sinn und die Durchführbarkeit logischer Überprüfungen neu überdacht werden.

Logische Plausibilitätsprüfungen dienen u.a. dazu, alle unerwünschten (Falsch-)Eingaben zu erkennen und möglichst zurückzuweisen. Die Integrität des Datenbestandes soll sowohl gegen die Eingabe unrichtiger Daten als auch in bestimmten Fällen gegen die Manipulation vorhandener richtiger Daten geschützt werden. Der Einbau von Plausibilitätsprüfungen in die entsprechenden Programme kann dafür auch weiterhin von Bedeutung sein. Allerdings muß vermieden werden, daß durch den Einsatz solcher Prüfungen das Programm künstlich aufgebläht und unübersichtlich wird sowie zur Leistungsverminderung des Rechners führt. Es empfiehlt sich, in Absprache mit der Fachabteilung, nur die notwendigen Plausibilitätsprüfungen programmtechnisch durchzuführen und die logischen Prüfungen dem Sachbearbeiter zu überlassen.

Für den Einsatz logischer Plausibilitätsprüfungen zur Vermeidung von duplizierten Datensätzen besteht keine Notwendigkeit mehr, da die modernen Datenbanksysteme Doppel-Einträge erkennen und zurückweisen (z.B. mit der Nachricht: „Datensatz bereits vorhanden").

Das Weglassen (unnötiger) logischer Plausibilitätsprüfungen steht nicht im Widerspruch zum Datenschutz, da bei jeder Maßnahme der Aufwand dem Nutzen gegenüberzustellen ist. Vollständige logische Plausibilitäten sind nur über kostspielige Expertensysteme zu erreichen.

22.3.8 Software-Entwicklung durch private Dritte

Nahezu jede Dienststelle bedient sich heute bei der Abwicklung ihrer Aufgaben der automatisierten Datenverarbeitung. Aus Wirtschaftlichkeitsgründen kann sich allerdings nicht jede Dienststelle eine eigene Programmierabteilung leisten, sondern muß Externe mit der Erstellung von Software beauftragen. Bei meinen Kontrollen und Beratungen wird mir häufig die Frage gestellt, was aus datenschutzrechtlicher Sicht bei der Software-Entwicklung durch private Dritte zu beachten ist, insbesondere dann, wenn die speichernde Stelle sensitive Daten verarbeitet.

Werden bei der Software-Entwicklung und -Wartung durch private Dritte personenbezogene Daten verwendet, handelt es sich um eine Form der **Auftragsdatenverarbeitung** im Sinne des Art. 3 BayDSG (bzw. § 11 BDSG). Danach hat der Auftraggeber den Auftragnehmer (Software-Ersteller) unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen auszuwählen. Die beauftragende Behörde bleibt als „Herr der Daten" für die Zulässigkeit und datenschutzgerechte Durchführung der DV-Verarbeitung verantwortlich und muß dafür Sorge treffen, daß die bei der Programmentwicklung benutzten personenbezogenen Daten nur entsprechend ihrer Weisung verarbeitet werden. Medizinische Daten und Steuerdaten unterliegen besonderen Geheimhaltungspflichten und dürfen Privaten nicht offenbart werden. Für den Fall, daß eine Offenbarung gegenüber privaten Dritten nicht zu umgehen ist, beispielweise um einen schwerwiegenden Programmfehler zu finden, müssen die Betroffenen nach dem Verpflichtungsgesetz auf die Einhaltung der Geheimhaltungsvorschriften verpflichtet werden. Zuwiderhandlungen sind dann unter Strafe gestellt.

Die Programmentwicklung — die zumeist außer Haus erfolgt — sollte grundsätzlich nur mit sogenannten **Testdaten** vorgenommen werden. Vor der Übernahme eines Programmes in den Echtbetrieb ist es aber üblich, den Abschlußtest mit echten (personenbezogenen) Daten durchzuführen. Ein solcher Test muß **vor Ort** im Beisein der Fachabteilung stattfinden, um einen unbefugten Datenzugriff durch externe Dritte auszuschließen. Unterliegen personenbezogene Daten einer besonderen Geheimhaltungspflicht, ist zu prüfen, ob und unter welchen Bedingungen diese Daten außer Haus verarbeitet werden dürfen. Für die Fehlerbehebung auch im Rahmen der Software-Fernwartung sind im Einzelfall geeignete Maßnahmen zu treffen, die die Geheimhaltung offenbarter Daten sicherstellen.

Bei einer Software-Entwicklung sind u.a. folgende Punkte zu beachten:
- Detaillierte schriftliche vertragliche Vereinbarungen
- Verbindliche Vorgaben (Pflichtenheft) für die einzuhaltenden Sicherheitsmaßnahmen
- Freigabeverfahren unter Federführung der auftraggebenden Stelle
- Festlegung der Sicherheitsmaßnahmen bei einer Software-Wartung
- Festlegung von Art und Umfang der Programmdokumentation und deren Aktualisierung
- Hinterlegung des Programmcodes mit entsprechender Dokumentation bei einer vertrauenswürdigen Stelle, soweit die speichernde Stelle den Programmcode aus urheberrechtlichen Gründen nicht selbst erhalten kann
- Genaue Dokumentation der Versionsstände der eingesetzten Software
- Bereitstellung eines Testdatenbestandes, der keinen Hinweis auf echte Daten gibt.

Im übrigen verweise ich auf eine entsprechende Orientierungshilfe (Notfallmaßnahmen bei Inanspruchnahme von DV-Dienstleistungen), die bei meiner Geschäftsstelle angefordert werden kann (siehe auch Nr. 22.1.5 im 12. Tätigkeitsbericht).

22.3.9 Zusammenarbeit mit der AKDB

Im Berichtszeitraum hat die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB), die die überwiegende Anzahl der kommunalen Gebietskörperschaften Bayerns mit automatisierter Datenverarbeitung versorgt, auf meine Anregungen hin die Anwender auf die beim Betrieb der Datenverarbeitung notwendigen Sicherheitsmaßnahmen hingewiesen. Ein erster Schritt war die Erstellung von sog. Kunden-Infos zum Thema „Datenschutz und Datensicherheit". Die Anwender von Siemens-Mehrplatzsystemen, von Digital-Kienzle-Systemen 9000 und von HP3000-Systemen haben solche Orientierungshilfen erhalten. In diesen Orientierungshilfen befinden sich Vorschläge über die Verbesserung der Systemsicherheit, wie automatische Deaktivierung von Bildschirmarbeitsplätzen und erweiterte Zugriffsschutzfunktionen. Darüber hinaus werden für die HP3000-Anwender zusätzliche Anregungen für den Datenschutz durch Einsatz von speziellen Sicherheitsprodukten gegeben.

Schließlich entwickelt die AKDB ein Notfallkonzept für HP3000-Anwender. Zusammen mit dem Herstel-

ler wird für interessierte Kunden ein Notfallkonzept erarbeitet, das eine Sicherheitsanalyse, einen Notfallplan und im Bedarfsfall die Bereitstellung eines Containerrechenzentrums einschließt.

23. Datenschutzregister

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

Wegen der Vielzahl der inzwischen angemeldeten Dateien und des begrenzten Nutzens der Übersicht für den Bürger wurde 1984 letztmalig eine Übersicht des Gesamtinhalts des Datenschutzregisters veröffentlicht. Auch der Umfang der Nachträge hat sich wegen der starken Ausweitung der automatisierten Datenverarbeitung von Jahr zu Jahr vergrößert und füllt inzwischen ebenfalls weit über 100 DIN-A4-Druckseiten pro Jahr.

Der 7. Nachtrag vom 4. November 1991 (Beilagen zum Bayer. Staatsanzeiger Nr. 47/48) enthält die Meldungen automatisierter Dateien von speichernden Stellen, die vom 10. November 1990 bis 11. Oktober 1991 in meiner Geschäftsstelle eingegangen sind.

Am 9. November 1990 umfaßte das gesamte Datenschutzregister 20.758 Dateien von insgesamt 6.073 speichernden Stellen. Zum Stichtag des 7. Nachtrags waren zum Datenschutzregister 22.391 Dateien von 6.927 speichernden Stellen gemeldet. Die Zunahme ist vor allem auf den vermehrten Einsatz von Arbeitsplatzcomputern im Schulbereich zurückzuführen.

Die Zahl der Bürger, die sich jährlich an mich wenden, um zu erfahren, in welchen Dateien Daten über sie gespeichert sein können, ist im Berichtszeitraum **stark zurückgegangen**. Bei einer Anfrage erhält der Auskunftssuchende, bezogen auf seinen Wohnsitz, einen Auszug aus der Übersicht zum Datenschutzregister über alle Stellen, deren Zuständigkeitsbereich sich auf seinen Wohnsitz erstreckt. Der Auszug enthält neben dem Namen und der Anschrift der Behörde die Art der Datei in einer Form, die ihm die Feststellung ermöglicht, ob er in dieser Datei gespeichert sein kann.

Die Pflege des Datenschutzregisters umfaßte im Berichtszeitraum folgende Arbeiten:

Neueintrag einer Stelle	894
Neueintrag einer Datei bei einer speichernden Stelle	2.248
Änderung bei der Bezeichnung einer speichernden Stelle	137
Dateibezogene Änderungen	27
Löschen einer speichernden Stelle	40
Löschen einer Datei	615

Die hohe Zahl der neueingetragenen Stellen ist dadurch zu erklären, daß im Bereichtszeitraum alle Schulen durch das Kultusministerium aufgefordert wurden, ihrer Meldepflicht nachzukommen. Außerdem wurden in diesem Jahr erstmals die Meldungen der Notare über deren personenbezogene Büroanwendungen berücksichtigt. Dabei handelt es sich um die automationsunterstützte Führung der Urkundenrolle, des Kostenregisters, des Erbvertragsverzeichnisses und des Massenbuches. Die verhältnismäßig hohe Anzahl von Dateilöschungen ist auf die Zusammenfassung von Einzeldateien zurückzuführen.

Die Führung des Datenschutzregisters beim Landesbeauftragten für den Datenschutz hat sich bewährt. Das Register gewährleistet für den Datenschutzbeauftragten den Überblick über die automatisiert betriebenen Dateien und für die Bürger die erforderliche Transparenz.

24. Datenschutz beim Bayer. Rundfunk (BR)

Bericht des Rundfunkbeauftragten

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

Bei der Überwachung der Datenverarbeitung des BR im Zeitraum vom 01.01. bis 31.12.1990 hat der Datenschutzbeauftragte — wie auch in den Vorjahren — keine datenschutzrechtliche Beanstandung ausgesprochen.

Der Datenschutzbeauftragte schildert die Entwicklung des Datenschutzrechts im Bereich des Rundfunks anhand des am 1.6.1991 in Kraft getretenen Bundesdatenschutzgesetzes, des novellierten Berliner und Hamburgischen Datenschutzgesetzes, der Entwicklung des Datenschutzes im Beitrittsgebiet und des Entwurfs einer EG-Datenschutzrichtlinie.

Eine zentrale Bedeutung für den Datenschutz bei Bundesrundfunkanstalten kommt dem Bundesdatenschutzgesetz zu. Das sogenannte „Medienprivileg" sei begrifflich präzisiert worden, inhaltlich würden jedoch, wie bisher, Daten, die von den Bundesrundfunkanstalten „ausschließlich zu eigenen journalistisch-redaktionellen Zwecken" verarbeitet oder genutzt werden, weitestgehend vom Geltungsbereich des neuen BDSG ausgenommen. Kehrseiten des Medienprivilegs seien die hinzugekommenen gesetzli-

chen Pflichten, Gegendarstellungen zu den gespeicherten Daten zu nehmen und in bestimmten Fällen Auskünfte über die einer Berichterstattung zugrundeliegenden personenbezogenen Daten zu erteilen. Neu sei ebenfalls die gesetzliche Institutionalisierung der unabhängigen Beauftragten für den Datenschutz bei den Bundesrundfunkanstalten anstelle des bisher zuständigen Bundesbeauftragten für den Datenschutz. Der Datenschutzbeauftragte hält es für wünschenswert, wenn die Vorbildfunktion des Bundesdatenschutzgesetzes insbesondere bezüglich des unabhängigen Datenschutzbeauftragten bei den Landesrundfunkanstalten wieder überall zum Tragen käme. So bedauert der Datenschutzbeauftragte, daß ähnlich wie auch in Bremen und Hessen, die Zuständigkeit des Berliner Datenschutzbeauftragten durch das seit November 1990 geltende, geänderte Berliner Landesdatenschutzgesetz auf den SFB ausgedehnt wurde. Der Datenschutzbeauftragte des SFB bleibe nur mehr für den ausschließlich journalistisch-redaktionellen Bereich zuständig. Beim neuen Hamburger Datenschutzgesetz, das am 01.08.1990 in Kraft getreten ist, sei dagegen die Kontrolle des Datenschutzbeauftragten durch einen unabhängigen Rundfunkdatenschutzbeauftragten beibehalten worden. Der Datenschutzbeauftragte schildert weiter, daß sich der Arbeitskreis der Rundfunkdatenschutzbeauftragten mit bereichsspezifischen Datenschutzregelungen im Bereich des Rundfunks in den neuen Bundesländern befaßt habe. Der erarbeitete Entwurf sichere das Medienprivileg für die neu zu schaffenden Rundfunkanstalten und die autonome Kontrolle des Datenschutzes durch einen speziellen Rundfunkdatenschutzbeauftragten. Darüber hinaus soll dem durch eine Berichterstattung Betroffenen unter gewissen Umständen ein Auskunfts- und Berichtigungsanspruch eingeräumt werden. Bezüglich einer von der EG-Kommission vorgelegten Datenschutzrichtlinie legt der Datenschutzbeauftragte dar, daß infolge eines Vorbehalts für nationale Regelungen im Medienbereich das Medienprivileg in der Bundesrepublik Deutschland aufrechterhalten werden könne.

Zum Datenschutz im BR berichtet der Datenschutzbeauftragte, daß die von ihm geforderte Datenschutz-Richtlinie für dezentrale DV-Anlagen vom Organisationsreferat erarbeitet worden sei und der Personalabteilung zur Einleitung des Mitbestimmungsverfahrens beim Personalrat vorliege. Eine Dienstanweisung für die dezentrale elektronische Personaldatenverarbeitung sei von der Personalabteilung, dem Organisationsreferat und ihm ausgearbeitet worden. In mehreren Bereichen des BR würden mittlerweile Personalcomputer zur Verarbeitung personenbezogener Daten, wobei es sich regelmäßig um Daten von Mitarbeitern handle, eingesetzt. Datenschutzrechtliche Fragen würden jeweils unter Beteiligung des Personalrats, des Organisationsreferats, der betroffenen Abteilung und ihm ausführlich besprochen und einvernehmlich gelöst. Den Bedenken, die der Datenschutzbeauftragte in seinem letzten Bericht gegen einen Online-Anschluß eines PC's der internen Revision an die Zentral-EDV erhoben hatte, habe der Intendant zwischenzeitlich Rechnung getragen und angewiesen, von einem Anschluß des PC's an die Zentral-EDV abzusehen.

Zur Einführung eines digitalisierten Fernmeldenetzes beklagt der Datenschutzbeauftragte, daß die Kontakte mit dem Bundesminister für das Post- und Fernmeldewesen zur Verbesserung des Informantenschutzes bei einem Anschluß der Rundfunkanstalten an das ISDN-Netz unbefriedigend verlaufen seien. Er äußert die Befürchtung, daß infolge der vorgesehenen Vollspeicherung der Verbindungsdaten für 80 bis 100 Tage eine Beschlagnahme von Telefondaten durch die Strafverfolgungsorgane erfolgen könne. Auch gegen die durch das ISDN-Netz ermöglichte Anzeige der Rufnummer des Anrufenden beim Angerufenen erhebt er Bedenken.

Zum Datenschutz im Personalbereich berichtet der Datenschutzbeauftragte, daß der Entwurf einer Rechtsverordnung zu § 93 a AO, mit der die Praxis der Kontrollmitteilungen der Rundfunkanstalten über die Empfänger von Honorarzahlungen an die Finanzämter eine ausdrückliche Rechtsgrundlage erhalten sollte, noch nicht in Kraft getreten sei. Er ist der Auffassung, die bisherige Praxis der Kontrollmitteilungen sei dennoch zulässig, da auf die subsidiären datenschutzrechtlichen Vorschriften als Rechtsgrundlage für die Datenübermittlung zurückgegriffen werden könne. Ich verweise hierzu auf meinen 12. Tätigkeitsbericht — 1990, Seite 39 f., wo ich dargestellt habe, daß das Finanzministerium allen Ministerien mitgeteilt hat, daß keine ausreichende Rechtsgrundlage für die allgemeine Übermittlung von Kontrollmitteilungen an die Finanzämter bestehe, solange die Verordnung zur Ausführung des § 93 a AO nicht ergangen ist. Den Datenschutzbeauftragten habe ich in einem Gespräch auf diese Rechtslage hingewiesen.

Die Probleme des Datenschutzes im Zusammenhang mit dem Medienprivileg greift der Datenschutzbeauftragte erneut auf. Er glaubt, daß die oben dargestellten Regelungen des neuen Bundesdatenschutzgesetzes zum Datenschutz bei Rundfunkanstalten — aus der Sicht der Kritiker des bisherigen Umfangs des Medienprivilegs — eine deutliche Verbesserung der Rechte der von einer Berichterstattung in ihren Persönlichkeitsrechten Betroffenen darstellen. Andererseits werde, weil die Rechte des Betroffenen auf Auskunft und Berichtigung erst nach einer Berichterstattung durch die Medien eingreifen, eine Vorzensur und Behinderung künftiger Berichterstattung weitestgehend vermieden. Gegen meine, bereits in mehreren vorherigen Tätigkeitsberichten dargestellten Auffassung zu einer Verbesserung des Datenschutzes im Medienbereich durch Einräumung von Rechten der

Betroffenen bereits vor einer Rechtsbeeinträchtigung, wendet sich der Datenschutzbeauftragte erneut. Er sieht dadurch die Funktionsfähigkeit der Medien und die Rundfunkfreiheit gefährdet.

Der Datenschutzbeauftragte berichtet weiter über die Schwierigkeiten der Ermittlung gebührenpflichtiger Autoradios. Die Verkehrsminister aus Bund und Ländern hätten erklärt, daß die Rundfunkanstalten bzw. ihre Beauftragten keine Auskünfte über die Halter von Kraftfahrzeugen aus dem Kraftfahrzeugregister zur Durchsetzung ihrer Rundfunkgebührenansprüche erhalten könnten. Die Regelungen des Straßenverkehrsgesetzes enthielten keine dafür erforderliche Rechtsgrundlage. Als einziges, sehr aufwendiges und für alle Beteiligten unbefriedigendes und unzumutbares Verfahren zur Feststellung von Kraftfahrzeughaltern sieht der Datenschutzbeauftragte die Anzeige bei der zuständigen Ordnungswidrigkeitenbehörde zur Einleitung eines Ordnungswidrigkeitenverfahrens gem. Art. 9 Abs. 1 Nr. 1 Rundfunkgebührenstaatsvertrag gegen den der Rundfunkanstalt unbekannten Halter eines dem Kennzeichen nach bekannten Kraftfahrzeuges. Da die Rundfunkanstalt in Unkenntnis der Daten des Halters nicht wisse, ob es sich bei dem eingebauten Autoradio um ein gebührenpflichtiges, nicht gemeldetes Gerät handle oder ob es gemeldet oder als gebührenfreies Zweitgerät anzusehen sei, werde sich dies erst nach Durchführung der Ermittlungen der Ordnungswidrigkeitsbehörde ergeben. Dies bedeute, daß es in einer Vielzahl von Fällen von vornherein zu unbegründeten Anzeigen der Rundfunkanstalt komme. Ein solches Vorgehen halte ich, wie unter Nr. 20.2 dargestellt, mangels Vorliegens eines Anfangsverdachts für unzulässig. Der Datenschutzbeauftragte hat sich meiner Auffassung angeschlossen.

25. Der Beirat

Die Mitglieder des Beirats werden nach Art. 29 Abs. 2 BayDSG für 4 Jahre, die Mitglieder des Landtags für die Wahldauer des Landtags bestellt. Im Berichtszeitraum gehörten dem Beirat an:

Ordentliche Mitglieder	**Vertreter**
die Landtagsabgeordneten	
Franz Brosch	Dr. Hans Gerhard Stockinger
Alois Braun	Dr. Helmut Müller
Franz Meyer	Wilhelm Wenning
Markus Sackmann	Georg Grabner
Dr. Klaus Hahnzog	Armin Nentwig
Carmen König	Joachim Wahnschaffe
die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
für die Staatsregierung	
Alfons Metzger Ministerialdirigent im Bayer. Staatsministerium des Innern	Dr. Klaus Geiger Ministerialdirigent im Bayer. Staatsministerium der Finanzen
für die Sozialversicherungsträger	
Ludwig Bergner Erster Direktor der Landesversicherungsanstalt Oberbayern	Herbert Schmaus Verwaltungsdirektor beim AOK-Landesverband Bayern
für die Kommunalen Spitzenverbände	
Klaus Eichhorn Geschäftsführender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Hans Herlitz Direktor bei der Anstalt für Kommunale Datenverarbeitung in Bayern
für den Verband der Freien Berufe in Bayern e.V.	
Dr. med. Hans Braun Präsident des Verbandes der Freien Berufe in Bayern e.V. ab 2.5.1991 Erwin Stein, MdL Präsident der Steuerberaterkammer München	Winfried Wachter Präsidiumsmitglied des Verbandes der Freien Berufe in Bayern e.V.

Den Vorsitz im Beirat führt Franz Brosch, MdL. Stellvertreterin ist Carmen König, MdL.

Der Beirat befaßte sich in seinen vier Sitzungen am 23.4.1991, 2.7.1991, 15.10.1991 und 3.12.1991 insbesondere mit folgenden Themen:

- Beratung des 13. Tätigkeitsberichts
- Bericht über Prüfungen und Beanstandungen
- Reduzierte Mitteilungen aus Gewerbesteuermeßbescheiden an Gemeinden
- Terrorismusbekämpfung und Datenschutz
- Datenschutz bei TELEKOM
- Verwertung der Volkszählungsergebnisse durch die Gemeinden
- Bekämpfung des Terrorismus und der organisierten Kriminalität
- Automatisiertes Liegenschaftsbuch
- Datenschutz im Bayerischen Mediengesetz und in den Rundfunkstaatsverträgen
- Datenschutz im Bereich der Polizei (APIS, ZEVIS, KAN)
- Berichte von Arbeitskreisen und Datenschutzkonferenzen
- Befugnisse des Landesbeauftragten bei der Beratung des Haushalts.

26. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzbeauftragten des Bundes und der Länder trafen sich 1991 zu zwei Konferenzen sowie einer Sonderkonferenz. Erstmals nahmen daran auch Vertreter der neuen Länder teil.

Schwerpunkte der Erörterungen waren:

- Telekommunikation und Datenschutz
- Widerspruchsrecht gegen datenschutzrechtliche Kontrollen im Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes
- Stasiakten-Gesetz
- Vorschlag für eine Richtlinie des Rats zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (gemeinsame Stellungnahme)
- Datenschutzgesetzgebung und Stand des Aufbaus der Datenschutzbehörden in den neuen Ländern
- Novellierung der Abgabenordnung
- Datenschutz im Recht des öffentlichen Dienstes
- Geplante Datei „Gewalttäter und Sport"
- Fragen eines gesetzlich geregelten Arbeitnehmerschutzes.

Anlage 1: Beschluß der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29.01.1991 zum Vorschlag der Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

I.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.
Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1990 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.
Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.
Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.
2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.
3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.
4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des Einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen

selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.
6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt — betrachtet man ihre Struktur, Aufgaben und Kompetenzen — diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser — aus den nationalen Datenschutzorganen zusammengesetzten — „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.
7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.
Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.
Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 2: Entschließung der 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.
Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß umso konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.
In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z.B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschrei-

ben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.
Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. **Bewerbung um Einstellung in den öffentlichen Dienst**

   Es ist — für den Bewerber transparent — festzulegen,
   - welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
   - ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,
   - ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
   - daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. **Sicherheitsüberprüfung**

   Es ist bereichsspezifisch gesetzlich festzulegen,
   - wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
   - welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
   - wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
   - daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
   - daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.*)

3. **Ärztliche Untersuchung**

   Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,
   - unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
   - daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
   - wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,
   - wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
   - daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
   - daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecken dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
   - daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und — soweit erforderlich — nur tätigkeitsbezogene Risiken mitzuteilen hat,
   - daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. **Beihilfen**

   Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. **Personalinformationssysteme**

   Es muß dienstrechtlich gewährleistet sein, daß
   - automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z.B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,
   - alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,
   - Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.
Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

*) Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13.09.1985, 18.04.1986 und 22.03.1990 nimmt die Konferenz Bezug.