Bayerischer Landtag
11. Wahlperiode

Drucksache **11/4766**
18. 12. 87

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 – 510 – 10

München, 18. Dezember 1987

An den
Herrn Präsidenten
des Bayerischen Landtags
München

Neunter 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 neunten Tätigkeitsbericht.

Mit vorzüglicher Hochachtung

Sebastian Oberhauser

Neunter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum 1986/1987

Inhaltsübersicht

		Seite
1.	**Vorbemerkung**	4
1.1.	Wechsel im Amt des Landesbeauftragten für den Datenschutz	4
1.2.	Bestellung des neuen Landesbeauftragten für den Datenschutz in Bayern	4
1.3.	Aufgaben des Landesbeauftragten für den Datenschutz	4
1.4.	Prüfkompetenz des Landesbeauftragten für den Datenschutz	4
1.5.	Prüftiefe	5
1.6.	Lücken im Persönlichkeitsschutz gegenüber Rundfunk und Presse	5
1.7.	Fortsetzung des „bayerischen Wegs“	6
2.	**Gesundheit**	6
2.1.	AIDS	6
2.1.1.	Umgang mit AIDS-Daten am Gesundheitsamt	7
2.1.2.	AIDS-Tests in Krankenhäusern	10
2.1.3.	AIDS-Tests im öffentlichen Dienst	10
2.1.4.	Anonyme Meldungen nach der Laborberichtsverordnung der Bundesregierung	11
2.1.5.	Namentliche Meldepflicht für Infizierte und Kranke	11
2.1.6.	Allgemeine Reihenuntersuchungen, epidemiologische Untersuchungen nach dem Mikrozensus-Verfahren	12
2.1.7.	Berechtigungsscheine für kostenlose anonyme AIDS-Untersuchungen	12
2.2.	Datenschutz im Krankenhaus	12
2.2.1.	Datenerhebung bei der Krankenhausaufnahme	12
2.2.2.	Forschung mit Patientendaten im Krankenhaus	13
2.2.3.	Tumorzentrum München	13
2.2.4.	Zentrale onkologische Dokumentation der Bayerischen Landesärztekammer und der Kassenärztlichen Vereinigung Bayerns	13
2.2.5.	Datenerhebung für medizinische Forschung	14
2.2.6.	Datenerhebung für Forschungsprojekt „Rehabilitation von Krebskranken“	14

2.2.7. Weitergabe von Patientendaten an die European Dialysis and Transplant Association (EDTA) 14

3. Sozialbehörden 14

3.1. Entwicklung von einwandfreien Antragsformularen 14

3.2. Gemeinsame Stammdatenbankverwaltung von Sozial- und Jugendamt 15

3.3. Veröffentlichung von Sozialdaten in einem Leserbrief 15

3.4. Übermittlung von Anschriften von Erblindeten an Vereine für Blindenhilfe 15

3.5. Anonymisierung von Daten der Mutterschaft 15

3.6. Einschaltung einer Gemeinde in das Widerspruchsverfahren über einen Rentenbescheid 16

3.7. Mitteilungen der Gemeinde über Fremdenübernachtungen gegenüber der Landwirtschaftlichen Berufsgenossenschaft 16

3.8. Darf eine Sozialbehörde der Polizei das Erscheinen einer gesuchten Person mitteilen? 17

4. Polizei 17

4.1. Zur Lage des Datenschutzes 17

4.2. Schwerpunkte meiner Tätigkeit 17

4.3. Führung und Auswertung von kriminalpolizeilichen Sammlungen (KpS) 18

4.3.1. Kriminalaktennachweis (KAN) 18

4.3.2. Polizeipräsidium München 20

4.4. Prüfung beim Bayerischen Landeskriminalamt 21

4.5. Personengebundene Hinweise 22

4.5.1. Entwicklung 22

4.5.2. Problem der Datenorganisation 22

4.5.3. Speicherung von HIV-Infektionen im polizeilichen Informationssystem 23

4.6. Neuordnung der polizeilichen Meldewege . 24

4.7. Arbeitsdatei PIOS – Innere Sicherheit (APIS) 25

4.8. Weitere Einzelfragen 25

4.8.1. Personenkarteien strafbarer Homosexualität 25

4.8.2. Übermittlung von Sozialdaten an die Polizei 26

4.9. Bayerische Grenzpolizei 26

4.9.1. Personenkontrollen 26

4.9.2. Prüfung des Präsidiums der Bayerischen Grenzpolizei 27

5. Verfassungsschutz 27

5.1. Prüfungen beim Bayerischen Landesamt für Verfassungsschutz 27

5.2. Sicherheitsüberprüfungen in der Privatwirtschaft zum Zwecke des Sabotageschutzes . 29

5.3. Bereichsspezifische Datenschutzregelungen bei Nachrichtendiensten 30

6. Justiz 30

6.1. Überblick 30

6.2. Automatisierungsvorhaben 31

6.2.1. Errichtung eines länderübergreifenden staatsanwaltschaftlichen Informationssystems 31

6.2.2. Automationsunterstützung der Personalverwaltung 31

6.2.3. Sonstige Automatisationsvorhaben 31

6.3. Datenschutzrechtliche Prüfung einer Staatsanwaltschaft 32

6.4. Gesetzgebung 32

6.4.1. Strafprozeßordnung 32

6.4.2. Justizmitteilungsgesetz 33

6.4.3. Strafvollzugsgesetz 33

6.4.4. Schuldnerverzeichnis 33

7. Städte, Gemeinden, Landratsämter 33

7.1. Neuer Personalausweis, Doppelvergabe von Seriennummern 33

7.2. Unzulässige Verwendung von Steuerdaten für andere Zwecke der Gemeinde 34

7.3. Bekanntgabe des Bauherrn und Entwurfverfassers 35

7.4. Bekanntgabe von hypothekarischen Belastungen im Wertgutachten eines Gutachterausschusses 35

7.5. Verwendung gemeindlicher Unterlagen aus dem Melde- und Standesamt zur Anfertigung einer Ortsstudie 35

7.6. Bearbeitung der Beihilfeangelegenheiten durch den Personalsachbearbeiter 36

8. Einwohnermelderegister 36

8.1. Auskünfte aus dem Melderegister zur Feststellung von Schuldneradressen – Personenverwechslungen 36

8.2. Veröffentlichung des Zuzugs von Neubürgern im kommunalen Mitteilungsblatt 36

8.3. Auskunftsersuchen einer Krankenkasse zu Werbezwecken 37

8.4. Melderegisterauskünfte an politische Parteien und Wählergruppen durch ein Service-Rechenzentrum 37

8.5. Alters- und Ehejubiläen 38

8.6. Übermittlung von Meldedaten an Adreßbuchverlage 38

8.7. Übermittlung von Daten Deutscher, die auch eine fremde Staatsangehörigkeit besitzen, an Ausländerbehörden 38

8.8. Online-Zugriff auf Melderegisterdaten – Berücksichtigung des Grundsatzes der Erforderlichkeit 39

8.9. Anpassung der Datensätze für das Meldewesen an das Melderecht 39

8.10. Kennzeichnung von Einwohnern als Wohngeldempfänger im Meldedatensatz 39

8.11. Auskunftspflicht des Meldepflichtigen – Nachweis der Angaben 40

8.12. Auskünfte aus dem Melderegister an die gemeindliche Steuerstelle 40

9. Steuerverwaltung 40

10. Personalwesen 40

10.1. Einsichtnahme der Frauenbeauftragten in Personalunterlagen 40

10.2. Versendung eines Wählerbriefes an dienstliche Anschriften 41

11. Statistik 41

11.1. Volkszählung 1987 41

11.1.1. Beratung und Kontrolle in der Vorbereitungsphase 42

11.1.2. Kontrolle der Durchführung der Volkszählung 44

11.1.3. Tätigkeit des Datenschutzbeauftragten in der Abgabephase 48

11.1.4. Zur Wiederholungsbefragung 48

11.1.5. Kontrolltätigkeit beim Landesamt für Statistik und Datenverarbeitung 48

11.1.6. Resümee zum Datenschutz bei der Volkszählung 48

11.2. Mikrozensus 48

11.3. Erhebungen zur amtlichen Schulstatistik . . 48

12. Schule und Hochschule 49

12.1. Hochschulwesen 49

12.1.1. Datenschutzrechtliche Prüfung der Ludwig-Maximilians-Universität München 49

12.1.2. Automation in der Hochschulverwaltung (DIAPERS) 49

12.1.3. Änderung des Bayerischen Hochschulgesetzes 49

12.1.4. Einzelfälle 50

12.2. Schulwesen 50

12.2.1. Automatisierte Schülerdateien 50

12.2.2. Automatisierte Lehrerdateien 51

12.2.3. Schulstatistik 51

12.2.4. Einzelfälle 51

13. Archivwesen und Forschung 52

13.1. Archivgesetzgebung 52

13.2. Benutzung von Archivgut für Forschungszwecke 53

14. Straßenverkehr 53

14.1. Zentrales Verkehrsinformationssystem (ZEVIS) 53

14.2. Einzelfälle 53

15. Industrie- und Handelskammern 54

15.1. Datenerhebung durch die IHK für das Handelsregister 54

15.2. Aufbau einer bundesweiten IHK-Informationsdatenbank 54

16. Neue Medien 54

16.1. Bildschirmtext 54

16.2. Telekommunikationsdienste 55

16.3. Medienerprobungs- und -entwicklungsgesetz (MEG); Datenschutzfragen in der Praxis 55

17. Technischer und organisatorischer Bereich 56

17.1. Technische Grundsatzfragen 56

17.1.1. Sicherheit von Personal Computern 56

17.1.2. Sicherheit von Kommunikationsnetzen (Hacker-Problematik) 57

17.1.3. „Kompromittierende" Abstrahlung 57

17.1.4. Revision der automatisierten Datenverarbeitung 58

17.2. Prüfungstätigkeit 59

17.3. Sicherheitsmaßnahmen bei der Durchführung der Volkszählung 87 60

17.3.1. Grundsätze 60

17.3.2. Beratung und Kontrolle der Erhebungsstellen 60

17.4. Technische Einzelprobleme 61

17.5. Orientierungshilfen zur Datensicherung . . . 62

18. Datenschutzregister 62

19. Datenschutz beim Bayerischen Rundfunk . 63

20. Der Beirat 64

21. Behandlung des 8. Tätigkeitsberichtes im Parlament 65

22. Konferenz der Datenschutzbeauftragten . 66

1. Vorbemerkung

1.1. Wechsel Im Amt des Landesbeauftragten für den Datenschutz

Hervorstechendes Ereignis im Berichtszeitraum war der Wechsel im Amt des Landesbeauftragten für den Datenschutz in Bayern. Mein Vorgänger, Dr. Konrad Stollreither, ist mit Erreichen der Altersgrenze am 31.7.1987 nach neunjähriger Tätigkeit in den Ruhestand getreten. Aus diesem Anlaß haben ihm der Bayerische Ministerpräsident und der Bayerische Landtag für sein konsequentes Eintreten für den Datenschutz in Bayern Dank und Anerkennung ausgesprochen. Besonders hervorgehoben wurde, daß Dr. Stollreither den Erfolg nicht in medienwirksamer Konfrontation mit Staatsregierung und Behörden, sondern in konstruktiver, verständnisvoller Zusammenarbeit mit ihnen gesucht habe.

1.2. Bestellung des neuen Landesbeauftragten für den Datenschutz in Bayern

Auf Vorschlag des Ministerpräsidenten und mit Zustimmung des Bayerischen Landtags hat mich die Bayerische Staatsregierung mit Wirkung vom 1.8.1987 zum neuen Landesbeauftragten für den Datenschutz bestellt.

Ich habe dieses Amt nicht unvorbereitet übernommen. Seit meinem Eintritt in den Staatsdienst im Jahre 1970 habe ich die innere Verwaltung auf allen Ebenen kennengelernt. Nach kurzer Einarbeitung bei der Regierung von Oberbayern, mehrjähriger Tätigkeit im Staatsministerium des Innern und am Landratsamt Ebersberg sowie erneuter Beschäftigung bei der Regierung habe ich neun Jahre in der Bayerischen Staatskanzlei im Referat Bundesratsangelegenheiten an der Gesetzgebung des Bundes mitgewirkt. Dabei und während der letzten Jahre als stellvertretender Leiter der Rechtsabteilung der Staatskanzlei konnte ich einen guten Überblick über die gesamte Staatstätigkeit gewinnen. Frühzeitig habe ich auch das Spannungsfeld zwischen dem Datenschutz und den übrigen Staatsaufgaben kennengelernt und versucht, bei der Gewichtung der einzelnen Aufgaben Einseitigkeit, Ungleichgewichte und Übertreibungen in der einen wie in der anderen Richtung zu vermeiden. So war und ist es mir genauso fremd, den Datenschutz zu verabsolutieren, wie ich es für falsch und für das Gesamtwohl schädlich hielte, der Ordnungsaufgabe des Staates ohne Rücksicht auf das informationelle Selbstbestimmungsrecht des einzelnen einen über das notwendige Maß hinaus gehenden oder gar absoluten Rang einzuräumen. Diesem Grundsatz folgend werde ich mich als Datenschutzbeauftragter in Bayern für einen Datenschutz nach Maß und Vernunft einsetzen.

1.3. Aufgaben des Landesbeauftragten für den Datenschutz

Meine Aufgabe als Landesbeauftragter für den Datenschutz in Bayern sehe ich darin, ausgerichtet am Maßstab des Grundgesetzes, der Bayerischen Verfassung und des übrigen geltenden Rechts, neben anderen Institutionen und soweit möglich gemeinsam mit ihnen dafür einzutreten, daß der Schutz des einzelnen vor Mißbrauch seiner persönlichen Daten durch öffentliche Stellen gewahrt bleibt. Das bedeutet in erster Linie, daß der Datenschutzbeauftragte im Rahmen seiner ihm durch Gesetz zugewiesenen Kompetenzen in gesetzlich garantierter Unabhängigkeit die Einhaltung des geltenden Datenschutzrechts überwacht.

In diesem Zusammenhang möchte ich einem immer wieder aufkommenden Mißverständnis entgegentreten: Umfang, Gewicht und Intensität des Datenschutzes oder – dogmatisch richtiger – das Ausmaß, in dem „das Grundrecht auf informationelle Selbstbestimmung" im überwiegenden Allgemeininteresse durch Gesetz eingeschränkt ist, bestimmt nicht der Datenschutzbeauftragte, sondern der Gesetzgeber. Der Datenschutzbeauftragte hat dem Gesetzgeber hierzu Verbesserungsvorschläge zu unterbreiten, die er aufgrund seiner Erkenntnisse und Erfahrungen für angezeigt hält.

Selbstverständlich wird sich der Gesetzgeber an der richtungweisenden Rechtsprechung des Bundesverfassungsgerichts, nicht zuletzt am Urteil zum Volkszählungsgesetz von 1983 orientieren müssen. Angesichts der technischen und organisatorischen Möglichkeiten der automatisierten Datenverarbeitung, der raschen Abrufbarkeit und Verfügbarkeit sowie der umfassenden Verknüpfbarkeit aller über eine Person gespeicherten Daten gibt es heute kaum noch belanglose persönliche Daten. Jede Erhebung, Speicherung und Nutzung von personenbezogenen Daten bedarf daher als Eingriff in das Recht auf informationelle Selbstbestimmung einer gesetzlichen Grundlage. Doch dürfen – das haben Verfassungsrichter und auch jüngst der Bundespräsident betont – die Entscheidungen des Gerichts nicht überinterpretiert und bis in die letzten Formulierungen hinein als Evangelium betrachtet werden. Dem Gesetzgeber bleibt hinreichender Gestaltungsspielraum, um bei der Abwägung der unterschiedlichen Belange neben dem Persönlichkeitsrecht des einzelnen auch die Interessen der Allgemeinheit gebührend berücksichtigen zu können. Das muß auch gelten für die Frage, in welchen Fällen bereichsspezifische Regelungen der Datenverarbeitung notwendig sind und in welchen Fällen eine generalklauselartige Regelung in den Datenschutzgesetzen ausreicht, damit eine kaum noch überschaubare Normenflut vermieden werden kann. Dann dürfen aber auch verantwortungsbewußte Datenschützer nicht der Versuchung erliegen, angeblich gestützt auf die Rechtsprechung des Bundesverfassungsgerichts, gegenüber den Parlamenten überzogene Forderungen zu vertreten. Ich jedenfalls werde mich bemühen, dem Gesetzgeber nur Vorschläge zur Verbesserung des Datenschutzes zu unterbreiten, die das Persönlichkeitsrecht des einzelnen stärken, ohne jedoch die überwiegenden Interessen des Allgemeinwohls zu beeinträchtigen.

1.4. Prüfkompetenz des Landesbeauftragten für den Datenschutz

Wie in anderen Ländern gab es auch in Bayern mit der Staatsregierung in den letzten Jahren Meinungsverschiedenheiten über den Umfang der Prüfkompetenz des Datenschutzbeauftragten. Dabei ging es vor allem um die Frage, ob der Datenschutzbeauftragte nach dem geltenden Bayerischen Datenschutzgesetz nicht nur die Datenverarbeitung in Dateien, sondern auch den Schutz von Daten, die nur in Akten verarbeitet werden, zu überwachen habe.

Zwar hat der Bayerische Datenschutzbeauftragte in der Regel nicht von sich aus Akten überprüft. Wenn allerdings in Eingaben von Bürgern ausnahmsweise einmal die Datenver-

arbeitung in Akten gerügt war, hat er auch Akten eingesehen.

Zur Frage der Prüfkompetenz hat schließlich die Bayerische Staatsregierung am 19.5.1987 folgenden Beschluß gefaßt:

> „Der Landesbeauftragte für den Datenschutz hat die Aufgabe, bei allen öffentlichen Stellen den Datenschutz beim Umgang mit personenbezogenen Daten in Dateien zu überwachen. Die Erfüllung dieser Aufgabe ist in vollem Umfang gewährleistet. Soweit es im Interesse einer effektiven Dateikontrolle notwendig ist, hat der Landesbeauftragte Einsicht in die dazugehörigen Akten. Den Nachweis der Notwendigkeit hat der Landesbeauftragte zu erbringen."

Ich habe schon vor meiner Bestellung zum Landesbeauftragten als stellvertretender Leiter der Rechtsabteilung der Staatskanzlei diese Auffassung der Staatsregierung geteilt, weil sie dem Wortlaut, Sinn und Zweck des Bayerischen Datenschutzgesetzes und den Intentionen des Gesetzgebers beim Erlaß des Gesetzes am ehesten entspricht. Auch die Gesetzeslage in den übrigen Ländern bestätigt diese Auffassung. Meine Bestellung zum Datenschutzbeauftragten konnte für mich selbstverständlich kein Anlaß sein, meine Meinung zu revidieren.

Auf die Praxis des Datenschutzbeauftragten hat sich der Beschluß der Staatsregierung vom 19.5.1987 nur wenig ausgewirkt. Der weit überwiegende Teil der Eingaben betrifft Beschwerden über die Datenverarbeitung in Dateien. Ihr Anteil wird mit dem unaufhörlichen Vordringen der automatisierten Datenverarbeitung weiter zunehmen. In den allerwenigsten Eingaben ist zudem ein Dateibezug von vornherein ausgeschlossen. Nur in diesen Fällen weise ich die Beschwerdeführer darauf hin, daß ich zur Prüfung nicht zuständig bin und lege ihnen nahe, die Angelegenheit von der Aufsichtsbehörde oder vom Ministerium überprüfen zu lassen. Stellt sich erst aufgrund der bei der Behörde eingeholten Stellungnahme heraus, daß es sich um keine Datenverarbeitung in Dateien handelt, wird der Bürger entsprechend unterrichtet. Halte ich aber die Sachbehandlung durch die Behörde für unrichtig, lege ich dem Bürger nahe, die Angelegenheit von der übergeordneten Behörde überprüfen zu lassen und unterrichte diese von dem Vorgang.

Im übrigen lege ich meine Kompetenz zur Überprüfung der Datenverarbeitung in Dateien dem Sinn und Zweck meiner Prüfkompetenz entsprechend weit aus. Unter meine Prüfkompetenz rechne ich nicht nur die Erhebung, Speicherung, Nutzung und Löschung von Daten in Dateien, sondern auch die Verarbeitung solcher Daten, die über Dateien erschlossen werden. Denn auch für diese Fälle gilt schließlich die Intention des Gesetzgebers, wegen der raschen Erschließbarkeit und erleichterten Nutzung dieser Daten eine besondere Schutzeinrichtung zu schaffen.

In keinem einzigen Fall haben sich zu diesen Fragen bisher Meinungsverschiedenheiten mit den kontrollierten Behörden ergeben.

1.5. Prüftiefe

Nach meinen persönlichen Erfahrungen in den ersten Monaten meiner Tätigkeit gibt es nicht selten Meinungsverschiedenheiten zwischen dem Datenschutzbeauftragten und den kontrollierten Behörden über die Erforderlichkeit, Zweckmäßigkeit und Nützlichkeit von Datenerhebungen, Speicherungen und Weitergaben sowie über den richtigen Zeitpunkt der Löschung von Eintragungen. Hier muß die unterschiedliche Aufgabenstellung von Datenschutzbeauftragtem und kontrollierten Fachbehörden gesehen werden.

Bei der Kontrolle behördlicher Datenverarbeitung hat der Datenschutzbeauftragte zwar die Befugnis zu voller rechtlicher Nachprüfung. Er hat allerdings in diesem Rahmen den Beurteilungsspielraum der Behörde bei Entscheidungen wertenden Inhalts und den behördlichen Ermessensrahmen zu beachten. Er kann und darf nicht etwa der Polizei die auf besondere Fach- und Sachkompetenz gegründete Verantwortung für die Erfüllung ihrer Sicherheitsaufgaben abnehmen und seine Wertung und Beurteilung an die Stelle derjenigen der Polizei setzen. Entscheidungen, die von der Polizei plausibel begründet werden und vertretbar erscheinen, kann der Datenschutzbeauftragte nicht beanstanden. Unberührt davon bleibt seine Aufgabe, immer wieder auf die Beachtung der Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und des geringstmöglichen Eingriffs hinzuwirken.

1.6. Lücken im Persönlichkeitsschutz gegenüber Rundfunk und Presse

In den letzten Jahren wurde der Schutz des Einzelnen gegen den Mißbrauch seiner persönlichen Daten durch den Staat beträchtlich verbessert. Die Datenschutzgesetze des Bundes und der Länder haben hieran maßgeblichen Anteil. Zahlreiche bereichsspezifische Datenschutzregelungen haben den Schutz der Persönlichkeit gegenüber behördlichen Eingriffen verstärkt. Durch die Rechtsprechung der Verfassungsgerichte ist der Gesetzgeber in Bund und Ländern aufgefordert, aus dem Grundrecht auf informationelle Selbstbestimmung Konsequenzen zu ziehen und – soweit noch nicht vorhanden – Rechtsgrundlagen für behördliche Eingriffe zu schaffen, die im überwiegenden Allgemeininteresse notwendig sind. Entsprechende Gesetzentwürfe sind in Vorbereitung. Auch die Datenverarbeitung in der Privatwirtschaft wurde 1978 im Bundesdatenschutzgesetz, wenn auch aus heutiger Sicht verbesserungsbedürftig, geregelt.

Einen weißen Fleck auf der Landkarte des Datenschutzes stellt nur noch der Medienbereich dar. Das Bundesdatenschutzgesetz schützt personenbezogene Daten nicht, die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden (§ 1 Abs. 3). Die Datenverarbeitung von Rundfunkanstalten sowie von Unternehmen der Presse und des Films wurde mit Rücksicht auf die im Grundgesetz verankerte Pressefreiheit (Art. 5 GG) in Erwartung einer Sonderregelung von den Vorschriften des Bundesdatenschutzgesetzes ausgenommen.

Dieses Privileg hat seinen Grund nicht darin, daß es im Medienbereich keines Datenschutzes bedürfte; im Gegenteil, namentlich Presse und Rundfunk speichern und verarbeiten personenbezogene Daten in besonders großem Umfang. Die tägliche Berichterstattung ist Datenverarbeitung. Rundfunk und Presse haben in den letzten Jahren gerade mit Hilfe der automatischen Datenverarbeitung riesige Pressedatenbanken angelegt, in denen über viele

Bürger teilweise sehr sensible personenbezogene Daten gespeichert sind. Unrichtige Speicherungen in den Pressedatenbanken können für die Bürger kaum weniger nachteilige Folgen haben als falsche Speicherungen in Behördencomputern.

Soweit Rundfunk und Presse personenbezogene Daten sammeln und zum Zweck der Veröffentlichung verarbeiten, bedarf es im Zeitalter der automatisierten Datenverarbeitung zum Schutz des Bürgers besonderer Regelungen, die einerseits die Pressefreiheit nicht in ihrem Wesensgehalt beeinträchtigen, andererseits aber das ebenfalls im Grundgesetz verankerte Persönlichkeitsrecht gewährleisten. Die allgemeinen zivilrechtlichen und die presserechtlichen Abwehransprüche reichen angesichts der möglichen Gefährdungen des Persönlichkeitsrechts durch Rundfunk und Presse nicht aus. Bund und Länder sind deshalb gefordert, in den Pressegesetzen unter Berücksichtigung des Grundrechts der Pressefreiheit wirksame Regelungen zum Schutz des Persönlichkeitsrechts der Bürger zu schaffen. Hierzu zählen vor allem Benachrichtigungspflichten, Auskunfts- und Berichtigungsansprüche für die Bürger und Löschungspflichten.

1.7. Fortsetzung des „bayerischen Wegs"

Wie oben bereits erwähnt, hat mein Vorgänger bei seiner Tätigkeit nicht die Konfrontation mit den kontrollierten Behörden, sondern die Zusammenarbeit mit ihnen gesucht. Der Erfolg nach neun Jahren gibt ihm Recht. Der Datenschutz ist in Bayern gewährleistet.

Bei meinen bisherigen Kontrollen wurde ich stets mit großer Offenheit und Aufgeschlossenheit aufgenommen. Nicht selten wird meine Geschäftsstelle in Einzelfragen des Datenschutzes um Rat gebeten. Gegenüber dem Datenschutzbeauftragten in Bayern wird nicht „gemauert", weil die kontrollierten Behörden wissen, daß sie wegen Fehler, die nun einmal vorkommen, nicht gleich zum Spott oder zur Ächtung durch das Publikum schonungslos an den Pranger gestellt werden.

Vor allem aber konnte ich mich bei meinen Antrittsbesuchen bei allen Kabinettsmitgliedern und den Amtschefs der bayerischen Ministerien davon überzeugen, daß ich bei meinem Bemühen um einen Datenschutz nach Maß und Vernunft mit ihrer vollen Unterstützung rechnen kann. Das ermutigt mich, den von meinem Vorgänger eingeschlagenen „bayerischen Weg" fortzusetzen.

2. Gesundheit

2.1. AIDS

Die meist tödliche Immunschwächekrankheit AIDS scheint eine der größten Herausforderungen unserer Gesellschaft in den letzten beiden Jahrzehnten des 20. Jahrhunderts zu werden. Der Verbreitungsgrad von AIDS ist wegen fehlender präziser epidemiologischer Unterlagen nur in groben Umrissen bekannt. Die Schätzungen über die Zahl der allein in der Bundesrepublik an HIV Infizierten bewegen sich zwischen 100.000 und 300.000. Bis zum Oktober 1987 wurden an das Bundesgesundheitsamt über 1.400 Erkrankungen gemeldet. Die Hälfte der Erkrankten ist bereits gestorben. Derzeit etwa alle acht bis zwölf Monate ist mit einer Verdoppelung der Erkrankungen zu rechnen. Die Infektionsgeschwindigkeit ist nicht bekannt. Hauptsächliche Übertragungswege sind Sexualkontakte und Blutkontakte von intravenös Drogenabhängigen (Fixern). Daneben sind aber auch andere Übertragungswege in der medizinischen Literatur beschrieben worden. Das besonders Tückische und Gefährliche an AIDS liegt darin, daß Infizierte jahre-, ja jahrzehntelang keine Krankheitssymptome zeigen und während dieser Zeit die Infektion weiterverbreiten.

AIDS ist nicht nur eine Krankheit von sog. Risikogruppen (u. a. Prostituierte und Fixer), unter denen sich die Infektion infolge ihres Sexualverhaltens und durch den Drogenkonsum begünstigt ausbreitet. AIDS droht inzwischen über diese Risikogruppen hinaus in die übrige Gesellschaft einzudringen.

Die Folgen von AIDS sind für die Betroffenen und die Gesellschaft katastrophal. Bei AIDS-Infizierten verläuft die Krankheit, die nach neueren Erkenntnissen bei mehr als der Hälfte der Infizierten innerhalb eines Zeitraumes von 10 Jahren nach der Infektion ausbricht, nach jämmerlichem Siechtum tödlich. Angesichts des vermuteten Verbreitungsgrades, der Ausbreitungsgeschwindigkeit und der Krankheitssymptome wird AIDS über viele Menschen, ihre Familien und über die ganze Gesellschaft unendliches Leid bringen. AIDS wird aller Voraussicht nach alle bisherigen Vorstellungen über die Kostenentwicklung im Gesundheitswesen sprengen. Die Angst des einzelnen vor der tödlichen Infektion mit AIDS könnte, wenn man diese Krankheit nicht alsbald in den Griff bekommt, das zwischenmenschliche Verhalten radikal verändern.

Hilfen der Medizin gegen die Ausbreitung von AIDS sind trotz erheblicher Anstrengungen auf absehbare Zeit nicht in Sicht. Angesichts des Ernstes der Bedrohung ist der Staat aus seiner verfassungsrechtlichen Verantwortung für Leben und Gesundheit seiner Bürger verpflichtet, alle zur Unterbrechung der Infektionsketten geeigneten Maßnahmen in Betracht zu ziehen. Die verfassungsrechtlich gebotene Abwägung zwischen dem Grundrecht der Nichtinfizierten auf Leben und Gesundheit und dem Selbstbestimmungsrecht der Infizierten wird regelmäßig zugunsten der Rechte der Nichtinfizierten ausfallen müssen.

Bei der Behandlung von AIDS stehen sich derzeit zwei Konzepte gegenüber:

1. Die Bundesregierung und ihr folgend die Mehrheit der Länder setzen in erster Linie auf Information und Beratung der Bevölkerung. Nur im äußersten Fall sollen auch hoheitliche Eingriffe nicht ausgeschlossen sein. Die Bundesregierung baut darauf, daß die angelaufene Aufklärungskampagne eine freiwillige grundlegende Änderung des Verhaltens der Bevölkerung, besonders der Risikogruppen, bewirken wird.

2. Das von der Bayerischen Staatsregierung entwickelte Konzept zur Bekämpfung von AIDS sieht ebenfalls umfassende Information und Beratung der Bevölkerung sowie Betreuung der Infizierten und Kranken vor. Gleichzeitig soll jedoch das bereits vorhandene seuchenrechtliche Instrumentarium angewandt und noch wirksamer ausgebaut werden.

   Am 25.2.1987 hat die Staatsregierung einen umfassenden Katalog von Maßnahmen zur Bekämpfung von AIDS beschlossen. In der Bekanntmachung vom 19.5.1987 hat

das Staatsministerium des Innern Hinweise für einen Vollzug des Seuchen-, Polizei- und Ausländerrechts gegeben.

Die bayerischen Maßnahmen, die ihre Rechtsgrundlagen im geltenden Bundes-Seuchengesetz haben, sehen im wesentlichen folgendes vor:

- Männliche und weibliche Prostituierte sowie intravenös Drogenabhängige (Fixer) gelten als „ansteckungsverdächtig" im Sinne des Bundes-Seuchengesetzes. Sie werden vierteljährlich vom Gesundheitsamt zu einem AIDS-Antikörper-Test vorgeladen. Die Vorladung erfolgt zunächst formlos. Wird ihr nicht Folge geleistet, so wird die betreffende Person förmlich vorgeladen und kann – im Weigerungsfalle – auch von der Polizei vorgeführt werden. Läßt sich der Ansteckungsverdacht im Gespräch mit dem Amtsarzt nicht ausräumen, so wird ein HIV-Antikörper Test durchgeführt. Nur im Falle der Weigerung wird die hierfür erforderliche Blutentnahme zwangsweise vorgenommen.

- Infizierte und Kranke werden verpflichtet, ihre Intimpartner sowie behandelnde Ärzte von der Infektion in Kenntnis zu setzen. Ihnen wird untersagt, Blut, Organe, Gewebe oder Samenflüssigkeit zu spenden. Infizierten Frauen wird verboten, Kinder zu stillen oder ihre Milch zu Ernährungszwecken abzugeben. Infizierten Prostituierten wird die Ausübung der Prostitution untersagt.

- Nach § 37 des Bundes-Seuchengesetzes können HIV-Infizierte, die nachweisbar uneinsichtig sind, weil sie wiederholt seuchenrechtlichen Anordnungen zuwider gehandelt haben und dadurch HIV weiterverbreiten oder andere gefährden, als letzte und schärfste Maßnahme abgesondert werden. Über die Absonderung, die regelmäßig nur auf Zeit erfolgt, entscheidet der Richter.

Die Umsetzung des bayerischen Maßnahmekatalogs erfordert, daß personenbezogene Daten erhoben und verarbeitet werden. So müssen die Gesundheitsämter Hinweisen über Ansteckungsverdächtige nachgehen. Diese Personen müssen sich einem AIDS-Test unterziehen. Ein positives Testergebnis ist ein hochsensibles Datum, weil es zahlreiche rechtliche Verpflichtungen gegenüber den Mitmenschen und der Gesellschaft begründet und auch einschneidende behördliche Maßnahmen nach sich ziehen, aber auch unangenehme Reaktionen des sozialen Umfelds auslösen kann. Negative Testergebnisse führen bei Angehörigen von Risikogruppen dazu, daß sie sich in regelmäßigen Abständen erneut einem Test unterziehen müssen.

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

Angesichts der Größe der Gefahr, die von AIDS dem einzelnen sowie Staat und Gesellschaft droht, hat sich der Landesbeauftragte für den Datenschutz gegenüber dem Staatsministerium des Innern zu den seuchen-, polizei- und ausländerrechtlichen Vollzugshinweisen des Staatsministeriums des Innern am 19.5.1987 folgendermaßen geäußert:

> „Der Katalog wurde datenschutzrechtlich in Einzelheiten von der zuständigen Abteilung des Staatsministeriums des Innern geprüft und für unbedenklich befunden. Aus der Sicht des Bayerischen Datenschutzbeauftragten bestehen keine Einwendungen gegen diese Feststellung.
>
> Wie in allen anderen Fällen empfiehlt der Datenschutzbeauftragte eine im speziellen gesetzliche Regelung und begrüßt die Absicht der Staatsregierung, im Bundesrat einen diesbezüglichen Gesetzentwurf einzubringen.
>
> Ebenfalls, wie in anderen Fällen, weist der Datenschutzbeauftragte darauf hin, daß mit diesen allgemeinen Feststellungen noch nichts über den künftigen datenschutzrechtlichen Vollzug im einzelnen ausgesagt ist."

Ich möchte diese Feststellungen meines Vorgängers nachdrücklich unterstreichen. Selbstverständlich sind auch bei der Bekämpfung von AIDS die verfassungsrechtlichen Grundsätze der Verhältnismäßigkeit, des geringstmöglichen Eingriffs und des mildesten Mittels zu beachten. An diesen Maßstäben müssen sich die Anti-AIDS-Konzepte der Bundesregierung wie der Staatsregierung messen lassen.

Im Hinblick auf die schwerwiegende Gefahr für die Gesundheit unseres Volkes sind seuchenrechtliche Maßnahmen nicht schon dann unzulässig, wenn sie als unangenehm empfunden werden oder behördliche Gesundheitskontrollen, ja sogar einschneidende Maßnahmen bis hin zur Absonderung mit sich bringen. Bedenken bestünden aber dann, wenn die Maßnahmen ungeeignet oder kontraproduktiv wären. Davon kann aber bei der Anwendung des seuchenrechtlichen Instrumentariums, das sich bei der Bekämpfung anderer Seuchen bewährt hat, keine Rede sein. Vielmehr werden an der Eignung der von der Bundesregierung eingeleiteten Maßnahmen, die weitgehend Einsicht und guten Willen der Betroffenen voraussetzen, angesichts der hauptsächlich betroffenen Personengruppen erhebliche Zweifel geäußert. Bei dieser Sachlage können die bayerischen Maßnahmen aus datenschutzrechtlicher Sicht nicht beanstandet werden.

2.1.1. Umgang mit AIDS-Daten am Gesundheitsamt

Auf der Grundlage des Maßnahmekatalogs der Bayerischen Staatsregierung zur Verhütung und Bekämpfung der Immunschwächekrankheit AIDS vom 25.2.1987 hat das Staatsministerium des Innern mit Bekanntmachung vom 19.5.1987 Hinweise zum Vollzug des Seuchen-, Ausländer- und Polizeirechts gegeben. Aus dieser Bekanntmachung wird deutlich, daß an den Gesundheitsämtern eine Reihe sensibler Daten über AIDS-verdächtige, -infizierte und -kranke Personen erhoben, gespeichert und an andere Stellen weitergegeben werden. Das konnte ich auch bei einem Informationsbesuch eines Gesundheitsamtes feststellen.

Die bei diesem Gesundheitsamt festgestellten Datenerhebungen, -speicherungen, -nutzungen und -übermittlungen begegnen keinen datenschutzrechtlichen Bedenken. Diese Maßnahmen sind durch die geltenden gesetzlichen Vorschriften gedeckt.

Da es sich bei den Daten über AIDS um besonders sensible Daten handelt, lege ich auf die Einhaltung des Datenschutzes in diesem Bereich besonderes Gewicht. Ich werde deshalb in nächster Zeit meine Kontrolltätigkeit auf diesem Gebiet bei den Gesundheitsämtern und Kreisverwaltungsbehörden, in den Krankenhäusern und bei der Polizei verstärken.

a) **Datenbestand über AIDS beim Gesundheitsamt**

Bei meinem Informationsbesuch eines Gesundheitsamtes habe ich festgestellt, daß zu AIDS folgende Daten vorhanden sind:

- Daten über AIDS-Erkrankungen,
- Daten über Krankheitsverdächtige,
- Daten über „Ausscheider" (Personen, die andere infizieren können, ohne bereits erkrankt oder krankheitsverdächtig zu sein),
- Daten über Ausscheidungsverdächtige (Annahme einer Infektion),
- Daten über Ansteckungsverdächtige (Personen, von denen anzunehmen ist, daß sie das HI-Virus aufgenommen haben, ohne krank, krankheitsverdächtig oder Ausscheider zu sein, z. B. Prostituierte, Fixer).

b) **Datenerhebung durch das Gesundheitsamt**

Nach § 31 BSeuchG wird das Gesundheitsamt nicht erst tätig, wenn jemand krank, krankheitsverdächtig, Ausscheider oder ausscheidungsverdächtig ist, sondern bereits bei Annahme eines Ansteckungsverdachts, d. h., wenn sich begründete Anhaltspunkte dafür ergeben, daß jemand der Prostitution nachgeht oder intravenös drogensüchtig (Fixer) ist.

Ein anonymer Hinweis reicht dem Gesundheitsamt für einen Ansteckungsverdacht genauso wenig aus wie z. B. eine Meldung, „eine Person sei in der Nähe der Toilette im Stachusuntergeschoß in München gesehen, Anbahnungsgespräche seien jedoch nicht beobachtet worden". Das Gesundheitsamt benötigt für seuchenrechtliche Maßnahmen nach §§ 31, 32 BSeuchG konkrete Anhaltspunkte für einen Ansteckungsverdacht.

Bei meinem Informationsbesuch konnte ich feststellen, daß das Gesundheitsamt seine Erkenntnisse aus folgenden Quellen schöpft:

- Betroffener

  Eine der zuverlässigsten Informationsquellen ist der Betroffene selbst.

  Das Gesundheitsamt hat aber nachdrücklich betont, daß Erkenntnisse aus einer anonymen Beratung in keinem Fall für eine seuchenrechtliche Maßnahme verwendet werden.

- Polizei oder Kreisverwaltungsbehörde

  Das Gesundheitsamt erhält regelmäßig Mitteilungen der Polizei über ihre Beobachtungen und Erkenntnisse sowie Informationen von der Kreisverwaltungsbehörde.

- Justiz

  Urteile zu Straftaten nach dem Betäubungsmittelgesetz werden nach der Anordnung über Mitteilungen in Strafsachen (MiStra) über das Staatsministerium des Innern, die Regierung und die Kreisverwaltungsbehörde an das Gesundheitsamt weitergeleitet.

- Blutspendedienst

  Blutspender unterziehen sich im Rahmen der Untersuchung ihres Blutes auch der AIDS-Untersuchung freiwillig. Aus der Sicht des Landesbeauftragten muß ein Blutspender über die weitere Verwendung eines positiven AIDS-Testergebnisses aufgeklärt werden. Nur wenn er zustimmt, kann ein positives Testergebnis dem Gesundheitsamt mitgeteilt werden.

- Angehörige, Bevölkerung

  Solche Mitteilungen sind nicht selten. Das Gesundheitsamt geht solchen Hinweisen mit der gebotenen Vorsicht nach.

- Gerichtsmedizin

  Bei Zwangsuntersuchungen auf Veranlassung des Gesundheitsamts meldet die Gerichtsmedizin das Ergebnis in Erfüllung des Untersuchungsauftrags.

- Psycho-soziale Betreuung

  Nimmt der Betroffene im Rahmen freiwilliger Beratung gem. Art. 11 des Gesundheitsdienstgesetzes die psycho-soziale Betreuung des Gesundheitsamts in Anspruch, gibt er seine Identität bekannt. Dann kann das Amt Namen und Anschrift sowie sonstige Angaben, die der Betroffene gemacht hat, speichern.

  Für seuchenrechtliche Zwecke dürfen Hinweise auf AIDS aus einer freiwilligen Beratung nach Art. 6 Abs. 2 Satz 2 des Gesundheitsdienstgesetzes innerhalb des Gesundheitsamtes nur dann weitergemeldet werden, wenn ein sogenannter Notstandsfall (§ 34 StGB) vorliegt, also die Abwehr von Gefahren für Leben oder Gesundheit Dritter die Meldung erfordert. In der Praxis wird jedoch eine solche Weitermeldung kaum vorkommen, da ein Betroffener, der sich der psycho-sozialen Betreuung unterzieht, auch für Vorsichtsmaßnahmen zum Schutze Dritter Einsicht zeigt und somit nach der Erfahrung des Gesundheitsamtes keinen Anlaß zu behördlichem Einschreiten gibt.

- Datenerhebungen aufgrund von eigenen Ermittlungen des Gesundheitsamtes nach den §§ 31 ff des Bundes-Seuchengesetzes

  Wenn jemand AIDS-krank, -krankheitsverdächtig, -ansteckungsverdächtig, Ausscheider oder ausscheidungsverdächtig ist, oder dies aufgrund von Tatsachen anzunehmen ist, stellt das Gesundheitsamt die erforderlichen Ermittlungen an, vor allem über Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit und der Infektion. Dies bedeutet: HIV-Verdächtige können vom Gesundheitsamt – notfalls auch zwangsweise – zu einem Aufklärungs- und Bera-

tungsgespräch vorgeladen werden, damit der Ansteckungsverdacht abgeklärt werden kann. Wenn der Ansteckungsverdacht im Gespräch nicht ausgeräumt werden kann, wird eine Blutuntersuchung durchgeführt. Die Blutprobe wird anonym an ein Testlabor versandt oder am Gesundheitsamt untersucht. Der Betroffene hat diese Maßnahmen nach dem Bundes-Seuchengesetz zu dulden. Das Ergebnis wird ihm in einem Beratungsgespräch eröffnet.

c) **Speicherung von AIDS-Daten beim Gesundheitsamt in Dateien:**

Meine Feststellung bei dem aufgesuchten Gesundheitsamt hat hierzu ergeben:

- Bei anonymer AIDS-Beratung findet eine Datenspeicherung nicht statt.
- Das Gesundheitsamt führt über die im Vollzug des Geschlechtskrankheitengesetzes erfaßten Prostituierten eine Kartei. Bei HIV-Positiven wird ein HIV-Vermerk angebracht.
- Außerdem wird ein HIV-Vermerk in der Blutspenderkartei des Blutspendedienstes, der zum Gesundheitsamt gehört, eingetragen.

Bei dem besuchten Gesundheitsamt wird hingegen noch keine AIDS-Datei oder AIDS-Kartei geführt, in der – getrennt nach Verdacht, Infizierung usw. – alle im Vollzug des BSeuchG dem Gesundheitsamt bekanntgewordenen mit AIDS belasteten Personen enthalten sind. Gegen eine solche Datei bestünden allerdings keine grundsätzlichen datenschutzrechtlichen Bedenken.

Zweifelsfreie Rechtsgrundlage für die Datenspeicherung ist Art. 16 Abs. 1 BayDSG i. V. mit § 10 Abs. 1 des Bundes-Seuchengesetzes. Die Speicherung ist zur rechtmäßigen Erfüllung der nach diesem Gesetz den Gesundheitsämtern zugewiesenen Aufgaben erforderlich.

d) **Datenübermittlung des Gesundheitsamtes an andere Stellen**

- Übersendung von Blutproben an das Landesuntersuchungsamt für das Gesundheitswesen

  Blutproben zum AIDS-Test werden an das Landesuntersuchungsamt für das Gesundheitswesen anonym übersandt. Der Landesbeauftragte für den Datenschutz hat das Landesuntersuchungsamt hinsichtlich des anonymisierten Verfahrens beraten und Unterlagen über die untersuchten Blutproben überprüft. Ich habe dabei festgestellt, daß keine Angaben gespeichert werden, die eine Reidentifizierung der gespeicherten Proben durch das Landesuntersuchungsamt erlauben würden.

- Datenübermittlung an die Kreisverwaltungsbehörde

  Die Ermittlungen gegen AIDS-verdächtige Personen führt das Gesundheitsamt (§§ 31 ff BSeuchG). Für die notwendigen Schutzmaßnahmen ist in Bayern die Kreisverwaltungsbehörde zuständig (§ 34 BSeuchG). Das Gesundheitsamt hat nach § 10 Abs. 6 BSeuchG der Kreisverwaltungsbehörde einen „Vorschlag" für erforderliche Maßnahmen zur Gefahrenabwehr zu übermitteln. Hierzu hat es an die Kreisverwaltungsbehörde auch die zur Durchführung der Maßnahmen erforderlichen Daten weiterzugeben.

  AIDS-Infizierte, bei denen das besuchte Gesundheitsamt nicht davon überzeugt ist, daß sie die entsprechenden Verhaltensmaßregeln des Gesundheitsamts freiwillig einhalten, werden der Kreisverwaltungsbehörde gemeldet, damit diese Maßnahmen nach dem Bundes-Seuchengesetz treffen kann. Ist das Gesundheitsamt der Auffassung, daß der Infizierte die Verhaltensmaßregeln freiwillig einhält, bespricht es den Fall mit der Kreisverwaltungsbehörde, zunächst ohne Namensnennung. Teilt die Kreisverwaltungsbehörde die Auffassung des Gesundheitsamtes nicht, werden die Daten personenbezogen an die Kreisverwaltungsbehörde übermittelt.

  Aber auch Personen mit negativem Testergebnis werden gemeldet, wenn sie weiterhin zum Kreis der Ansteckungsverdächtigen (Prostituierte, i.V. Drogenabhängige) gehören, damit die Kreisverwaltungsbehörde die notwendigen Wiederholungsuntersuchungen anordnen kann.

  An die Kreisverwaltungsbehörde werden keine Erkenntnisse aus der anonymen AIDS-Beratung weitergegeben.

- Datenübermittlung an die Ausländerbehörde

  Die Ausländerbehörde verlangt vor der erstmaligen Erteilung der Aufenthaltserlaubnis an Ausländer aus bestimmten Ländern eine ärztliche Bescheinigung. Nach der Bekanntmachung des Staatsministeriums des Innern vom 19.5.1987 ist auch eine Untersuchung auf eine HIV-Infektion vorzunehmen. Der Ausländer hat ein Gesundheitszeugnis vorzulegen. Dazu gehört auch der HIV-Test. Legt er ihn nicht vor oder ist der HIV-Test positiv, ergreift das Ausländeramt die im Ausländergesetz vorgesehenen Maßnahmen. Im übrigen gelten für Ausländer die Vorschriften des Bundes-Seuchengesetzes.

  Im Asylverfahren wird ein Test regelmäßig aufgrund Einwilligung des Asylbewerbers durchgeführt. Verweigert ein Bewerber die Untersuchung, so kann ihm die Ausländerbehörde nach Art. 20 Abs. 2 des Asylverfahrensgesetzes zur vorläufigen Aufenthaltsgestattung einen AIDS-Test zur Auflage machen. Diese Anordnung ersetzt die Zustimmung zum AIDS-Test. Bei AIDS-verdächtigen Asylbewerbern ist wiederum ein Zwangstest grundsätzlich möglich.

- Datenübermittlung an die Polizei zur Vollzugshilfe bei Anordnungen des Gesundheitsamtes

  Das Gesundheitsamt versucht zunächst, ohne Mitwirkung der Polizei einen AIDS-Verdacht zu klären. Erscheint eine vom Gesundheitsamt formlos angeschriebene Person nicht und folgt sie auch der Anordnung des Amtes nicht, kann das Amt die Polizei um Vollzugshilfe bitten. Das Verwaltungszustellungs- und Vollstreckungsgesetz (Art. 37 Abs. 2) sowie das Polizeiaufgabengesetz (Art. 2 Abs. 2, Art. 29) bieten hierfür die Rechtsgrundlagen. Die Polizei kann die Person auch zwangsweise vorführen, wenn sie der Vorladung nicht Folge leistet. Da bei zwangsweisen Vorführungen mit körperlicher Gegenwehr gerechnet

werden muß, weist das Gesundheitsamt die Polizei auf den AIDS-Verdacht und die mit Blutkontakten verbundene Infektionsgefahr hin.

Zur Vermeidung von Fehlinterpretationen durch die Polizei halte ich allerdings einen Hinweis für erforderlich, daß lediglich ein AIDS-Verdacht vorliegt. Selbstverständlich rechtfertigt ein solcher AIDS-Verdacht noch nicht die Eintragung eines personengebundenen Hinweises im Kriminalaktennachweis oder in der Fahndungsdatei. Dies ist nach meiner Auffassung erst zulässig, wenn die Polizei von der tatsächlich vorliegenden HIV-Infektion sichere Kenntnis erhält.

- Übermittlung der AIDS-Infektion an die Staatsanwaltschaft

  Der Staatsanwaltschaft hat das Gesundheitsamt nach § 161 StPO auf Anforderung alle zur Verfolgung von Straftaten erforderlichen Daten zu übermitteln. Dazu kann auch eine AIDS-Infektion gehören.

2.1.2. AIDS-Tests in Krankenhäusern

Unter Krankenhausärzten besteht erhebliche Unsicherheit über die Voraussetzungen unter denen ein AIDS-Test zulässig ist. Ein in der Fachpresse bekanntgewordenes strafrechtliches Ermittlungsverfahren gegen einen Arzt, der eine Blutprobe ohne Kenntnis des Patienten auf HIV testen ließ, wurde eingestellt.

Zur Beseitigung der rechtlichen Unklarheit, unter welchen Voraussetzungen HIV-Tests bei Krankenhauspatienten zulässig sind, hat der bayerische Staatssekretärausschuß AIDS den Krankenhausträgern die Aufnahme einer Einwilligungsklausel in die Krankenhausaufnahmeverträge empfohlen. Die AIDS-Klausel lautet:

„Der Patient ist mit einer Blutentnahme zum Zweck der Untersuchung auf das Vorliegen einer HIV-Infektion einverstanden, wenn diese Untersuchung aus ärztlicher Sicht angezeigt ist."

Das Staatsministerium für Wissenschaft und Kunst hat für die bayerischen Hochschulkliniken angeordnet, diese klarstellende Klausel in den Krankenhausvertrag aufzunehmen. Das Staatsministerium des Innern hat der Bayerischen Krankenhausgesellschaft die Verwendung der Klausel empfohlen.

Nach den Ausführungen der Fachbehörden wird die Durchführung von HIV-Tests und damit die Datenerhebung zu AIDS bei einer Krankenhausaufnahme in folgenden Fällen für notwendig erachtet:

- Wenn zur differenzialdiagnostischen Abklärung von Beschwerden als deren Ursache auch eine HIV-Infektion in Betracht kommt,
- wenn die Einbeziehung einer etwaigen Immunschwäche in die Beurteilung, ob eine bestimmte Therapie (insbesondere eine Operation) durchgeführt werden kann, erforderlich ist,
- wenn es zum Schutz des Krankenhauspersonals vor einer HIV-Infektion durch Nadelstich- u. a. Verletzungen oder Blut-Haut-Kontakte erforderlich ist.

Der Landesbeauftragte begrüßt die Klarstellung, wonach der Patient durch Unterschrift unter den Krankenhausvertrag sein Einverständnis mit dem HIV-Test, „wenn diese Untersuchung aus ärztlicher Sicht angezeigt ist", erklärt. Ein besonderes Aufklärungsgespräch ist nicht Bedingung für die Wirksamkeit der Einwilligung. Es sei denn der Patient wünscht ein solches Gespräch.

Gegen das Einholen des Einverständnisses des Patienten mit dem HIV-Test im Krankenhaus ist, wie aus einem anderen Bundesland bekannt wurde, eingewandt worden, bei den Patienten würden dadurch unnötig Angstgefühle erzeugt, da das Ergebnis des Tests nur in weniger als 1 % der Fälle HIV-positiv sei. Nach meiner Ansicht wird jedoch durch die in Bayern vorgesehene Einwilligungsklausel, die generell in den Aufnahmevertrag aufgenommen wird, eine Belastung des Patienten weitgehend vermieden. Wer auf der Basis der bayerischen Klausel sein Einverständnis erklärt, weiß, daß er nicht in jedem Fall, sondern nur dann auf AIDS getestet wird, wenn dies aus ärztlicher Sicht angezeigt ist. Er weiß zudem, daß eine entsprechende Erklärung jedem Patienten bei der Aufnahme vorgelegt wird, also nicht bereits sein spezieller Gesundheitszustand dazu führt, ihn um die Einwilligung in den Test zu bitten.

Selbstverständlich unterliegen AIDS-Tests der ärztlichen Schweigepflicht. Testergebnisse dürfen also nach den für dieses Institut geltenden Vorschriften nicht weitergegeben werden.

2.1.3. AIDS-Tests im öffentlichen Dienst

Bewirbt sich jemand um die Berufung in das Beamtenverhältnis, in das Richterverhältnis oder in den Anwärterdienst als Notarassessor, führen die Gesundheitsämter bei der Einstellungsuntersuchung einen HIV-Antikörper-Test durch. Die Blutprobe wird anonymisiert an das Landesuntersuchungsamt eingesandt. Die Bewerber werden von der personalbewirtschaftenden Stelle und vom untersuchenden Arzt des Gesundheitsamtes über den Zweck der Blutentnahme aufgeklärt.

Ein negatives Testergebnis wird nicht gesondert weitergeleitet. Es ist im Abschlußurteil über die „Eignung" enthalten.

Bei positivem Testergebnis leitet das Gesundheitsamt das erstellte Gesundheitszeugnis, das sich nur zur „Eignung" äußert, jedoch keine Diagnose enthält, dann an den Auftraggeber weiter, wenn der Betroffene sich ausdrücklich damit einverstanden erklärt. Lehnt er dies ab, teilt das Gesundheitsamt der personalbewirtschaftenden Stelle lediglich mit, das Gutachten könne wegen fehlender Einwilligung des Bewerbers nicht abgegeben werden.

Das Gesundheitsamt verwendet die Erkenntnisse, die es bei der Einstellungsuntersuchung gewinnt, nicht für andere Zwecke (Art. 6 und 7 des Gesetzes über den öffentlichen Gesundheitsdienst). Es belehrt und berät einen testpositiven Bewerber. Kommt es dabei freilich zur Überzeugung, daß der Betreffende uneinsichtig und unbelehrbar ist, muß es die notwendigen seuchenrechtlichen Maßnahmen in Erwägung ziehen (s. o. 2.1.1 Umgang mit AIDS-Daten am Gesundheitsamt).

Aus der Sicht des Datenschutzes bestehen gegen den AIDS-Test bei der Einstellungsuntersuchung, der nicht die Bekämpfung von AIDS zum Gegenstand hat, sondern sich

aus den beamtenrechtlichen Vorschriften ergibt, keine Bedenken.

Gemäß Art. 11 Abs. 1 Nr. 3 des Bayerischen Beamtengesetzes darf in das Beamtenverhältnis auf Lebenszeit nur berufen werden, wer sich in einer Probezeit hinsichtlich seiner Eignung, Befähigung und fachlichen Leistung bewährt hat. Unter dem Begriff der Eignung ist vor allem auch die gesundheitliche Eignung zu verstehen. Der Bewerber ist für die Übernahme in das Beamtenverhältnis auf Lebenszeit nicht erst bei Dienstunfähigkeit ungeeignet, sondern bereits dann, wenn wegen einer psychischen oder körperlichen Veranlagung nicht mit einem hohen Grad an Wahrscheinlichkeit eine vorzeitige Versetzung in den Ruhestand ausgeschlossen werden kann. Die gesundheitliche Eignung ist bereits bei der Einstellung in den Verwaltungsdienst und der Berufung in das Beamtenverhältnis auf Probe zu prüfen. Der Bewerber unterzieht sich der Untersuchung auf freiwilliger Basis. Von der einstellenden Behörde wird ihm zwar aufgegeben, sich zur Feststellung seiner Gesundheit einer ärztlichen Untersuchung zu unterziehen. Es wird damit aber noch keine beamtenrechtliche Verpflichtung für den Bewerber ausgelöst. Im Zeitpunkt der ärztlichen Untersuchung steht er der Einstellungsbehörde als Bürger gegenüber, der den aus dem Beamtenrecht sich ergebenden Verpflichtungen, die durch die Übernahme in das Beamtenverhältnis begründet werden, noch nicht unterworfen ist. Wendet er sich – aus welchen Gründen auch immer – gegen eine ärztliche Untersuchung, hier gegen eine Untersuchung auf AIDS, so ist es ihm unbenommen, sich diesen ärztlichen Feststellungen zu entziehen.

Für Angestellte und Arbeiter ist eine generelle Einstellungsuntersuchung wie bei Beamten nicht vorgesehen. Der Arbeitgeber kann nach den Tarifvorschriften nur verlangen, daß der Bewerber seine körperliche Eignung (Gesundheitszustand und Arbeitsfähigkeit) durch das Zeugnis eines vom Arbeitgeber bestimmten Arztes nachweist. Der Untersuchungsauftrag des Arbeitgebers beschränkt sich auf solche Feststellungen, die für die körperliche Eignung des Bewerbers im Hinblick auf die auszuübende Tätigkeit relevant sind. Die Tarifbestimmungen gestatten es dem öffentlichen Arbeitgeber nach Ansicht des für das Personalrecht federführenden Staatsministeriums der Finanzen somit nicht, generell einen AIDS-Test zu verlangen. Etwas anderes gilt selbstverständlich für Bewerber für bestimmte Funktionen, z.B. für Klinikpersonal.

2.1.4. Anonyme Meldungen nach der Laborberichtsverordnung der Bundesregierung

Am 1.10.1987 trat die Verordnung über die Berichtspflicht für positive HIV-Bestätigungstests (Laborberichtsverordnung) in Kraft. Am 1. Januar 1988 wird sie durch eine inhaltlich übereinstimmende Verordnung ersetzt, da die derzeitige Verordnung ohne Zustimmung des Bundesrates erlassen wurde und deshalb ihre Geltungsdauer auf 3 Monate begrenzt ist.

Zum Bericht verpflichtet sind nur Personen, die HIV-Bestätigungstests durchführen oder für die Durchführung verantwortlich sind. Diese technisch sehr aufwendigen Tests werden in Bayern derzeit nur in wenigen Labors vorgenommen. Dazu gehören das Hygieneinstitut der beiden Münchner Universitäten und die Landesuntersuchungsämter Nord- und Südbayern für alle Blutproben aus dem öffentlichen Bereich.

Die Berichte sind gegenüber dem Bundesgesundheitsamt abzugeben, das sie für epidemiologische Untersuchungen auswertet. Sie sind nur bei positiven Ergebnissen vorgesehen und dürfen weder den Namen noch Namensbestandteile oder eine Verschlüsselung zur Kennzeichnung der Person enthalten. Die Folge des Verzichts auf eine Codierung der Meldungen ist freilich, daß Mehrfachzählungen nicht ausgeschlossen werden können. Aus der Sicht des Datenschutzes wäre eine Codierung zulässig, wenn eine Reidentifizierung ausgeschlossen ist.

Der Laborbericht muß das Alter, das Geschlecht, die ersten beiden Ziffern der Postleitzahl des Wohnsitzes der untersuchten Person, Angaben über den Anlaß der Untersuchung, die mögliche Übertragungsweise, das vorliegende Krankheitsbild sowie darüber enthalten, ob die untersuchte Person schon als HIV-positiv bekannt war. Diese Angaben erfolgen nach dem Verordnungstext, soweit sie „dem zum Bericht Verpflichteten bekannt" sind.

Nach meinen bisherigen Erfahrungen steht zu befürchten, daß bei einem erheblichen Teil der Berichte diese Angaben fehlen werden, da zumindest die bayerischen Gesundheitsämter die Blutproben in der Regel nur mit einer Nummer versehen an die Landesuntersuchungsämter schicken.

Einen wirksameren Weg zur Erkennung von Mehrfachmeldungen schlägt der von der Bayer. Staatsregierung am 16.7.1987 vorgelegte Entwurf eines Gesetzes zur Änderung des Bundes-Seuchengesetzes vor. In § 9 a ist die Einführung einer anonymen codierten Berichtspflicht an das Bundesgesundheitsamt vorgesehen. Im Unterschied zur Laborberichtsverordnung der Bundesregierung soll beim bayerischen Vorschlag die Codierung sicherstellen, daß Doppelmeldungen festgestellt werden können und den zum Bericht verpflichteten Labors die Angaben mitgeteilt werden, über die sie berichten sollen.

2.1.5. Namentliche Meldepflicht für Infizierte und Kranke

Im bayerischen Gesetzentwurf zur Änderung des Bundes-Seuchengesetzes vom 16.7.1987 ist neben der vorgenannten anonymen und codierten Laborberichtspflicht auch eine namentliche Meldung solcher Infizierter und Kranker vorgesehen, die erkennen lassen, daß sie uneinsichtig sind und die Infektion fahrlässig oder vorsätzlich weiterverbreiten werden. Zur Meldung an das zuständige Gesundheitsamt wäre der behandelnde, nicht aber der sonst zugezogene Arzt (Konsiliararzt) verpflichtet.

Die Meldepflicht soll sich auf HIV-infizierte Personen beschränken, für die der durch T a t s a c h e n begründete Verdacht besteht, daß sie, trotz Belehrung, durch ihre Lebensweise oder ihre allgemeinen Lebensumstände eine Gefahr der Übertragung von HIV auf andere bilden. Eine solche Gefahr – und damit eine Meldepflicht des Arztes – liegt nach dem Gesetzentwurf vor allem dann vor, wenn tatsächliche Anhaltspunkte dafür bestehen, daß eine HIV-infizierte Person der Prostitution nachgeht oder mit Intravenös-Drogenabhängigen Injektionsbestecke gemeinsam benutzt. Gleiches soll gelten, wenn nur der Verdacht besteht, daß eine Person HIV-infiziert ist, sich aber weigert, eine Untersuchung auf HIV vornehmen zu lassen, und nicht ausgeschlossen werden kann, daß die Person durch ihre

Lebensweise oder ihre allgemeinen Lebensumstände eine Gefahr der Übertragung von HIV auf andere bilden kann.

Der Entwurf sieht die Meldung des Familien-, Vor- und Geburtsnamens, des Tages und Ortes der Geburt, der Anschrift, der derzeit ausgeübten Tätigkeit sowie des Anlasses für die namentliche Meldung vor. Gegebenenfalls umfaßt die Meldung auch die Mitteilung der Untersuchungsbefunde und der Untersuchungsstelle.

Der Gesetzentwurf knüpft die namentliche Meldepflicht damit an den begründeten Verdacht der Weiterverbreitung der Infektion in Fällen von festgestellter HIV-Infektion oder begründetem Verdacht einer HIV-Infektion. Allgemeine Vermutungen reichen hierfür nicht aus; die Beurteilung der allgemeinen Lebensumstände muß objektiv überprüfbar sein. Der Entwurf nennt als Beispiele für eine solche Weiterverbreitungsgefahr Prostituierte und Fixer.

Ich halte die Einführung einer Meldepflicht in dem vom Gesetzentwurf festgelegten Umfang datenschutzrechtlich für zulässig, zumal sie ausdrücklich auf Personen beschränkt ist, die aufgrund ihrer Uneinsichtigkeit eine mögliche Infektionsquelle darstellen. Der Schutz der nichtinfizierten Bevölkerung gebietet es zwingend, daß das Gesundheitsamt in die Lage versetzt wird, solche Fälle zu klären und unter Einschaltung der Kreisverwaltungsbehörde die notwendigen Maßnahmen zu ergreifen.

2.1.6. Allgemeine Reihenuntersuchungen, epidemiologische Untersuchungen nach dem Mikrozensus-Verfahren

Im Gegensatz zu anderen bekannten Infektionskrankheiten liegt die besondere Schwierigkeit bei der Feststellung des Umfangs der Ausbreitung von AIDS darin, daß die Krankheit meist erst Jahre nach der Infektion ausbricht. Das stellt die Gesundheitsbehörden bei der Ermittlung des Durchseuchungsgrades der Bevölkerung vor erhebliche Probleme. Die anonyme Laborberichtspflicht ist nur sehr eingeschränkt geeignet, den Behörden einen verläßlichen Überblick zu verschaffen, da nur ein Teil der Infizierten den AIDS-Test machen läßt. Zur Unterbrechung der Infektionskette ist die Laborberichtspflicht überdies ungeeignet.

Deshalb sind weitere Wege zur Feststellung des Durchseuchungsgrades und der Ausbreitungsgeschwindigkeit von AIDS erwogen worden.

Eine Reihenuntersuchung der gesamten Bevölkerung könnte zwar einen Überblick über die derzeitige Ausbreitung von AIDS verschaffen. Es dürfte allerdings mit erheblichen Schwierigkeiten verbunden sein, über 40 Millionen Deutsche und Ausländer von der Notwendigkeit eines AIDS-Tests zu überzeugen oder durch Verwaltungszwang zum Test zu veranlassen. Außerdem würde eine einmalige Reihenuntersuchung nach Schätzungen Kosten von etwa 800 Mio DM verursachen. Bei den heutigen Kenntnissen über AIDS dürfte eine Reihenuntersuchung außer Verhältnis stehen. Sollte jedoch das Vordringen von AIDS trotz konsequenter Anwendung aller (auch seuchenrechtlichen) Maßnahmen nicht aufzuhalten sein und diese Krankheit aus den Risikogruppen heraus in die allgemeine Bevölkerung vordringen, dann wird eine allgemeine Reihenuntersuchung nicht zu umgehen und im Hinblick auf den Grundsatz der Verhältnismäßigkeit auch zulässig sein. In diesem Fall wird man es aber kaum bei anonymen epidemiologischen Untersuchungen bewenden lassen können, sondern gegen die festgestellten Infizierten unter konsequenter Anwendung des seuchenrechtlichen Instrumentariums vorgehen müssen. Unter diesem Gesichtspunkt kommt schon heute der vollen Anwendung des Seuchenrechts auf die Risikoträger nicht zuletzt aus der Sicht des Datenschutzes überragende Bedeutung zu. Die Eingriffe in die Freiheit des einzelnen und das informationelle Selbstbestimmungsrecht werden um so tiefer und schwerer sein, je länger heute wirksame Maßnahmen hinausgeschoben werden.

Wenig brauchbare Aussagen zum Durchseuchungsgrad dürfte von Untersuchungen nach dem Mikrozensus-Verfahren zu erwarten sein. Im übrigen sind bisher nach dem Mikrozensus-Gesetz nur Daten erhoben worden, die dem zur Auskunft Verpflichteten bereits vorlagen, nicht jedoch Angaben, die erst aufgrund einer ärztlichen Untersuchung zu ermitteln waren. Schließlich dürften Personen, die für eine AIDS-Infektion völlig außer Betracht bleiben – das ist immer noch der weit überwiegende Teil der Bevölkerung – für die Vorladung zum AIDS-Test keinerlei Verständnis haben. An der allgemeinen Bevölkerung dürfen epidemiologische Zwangsmaßnahmen erst vorgenommen werden, nachdem die seuchenrechtlichen Maßnahmen gegen HIV-Infizierte und Risikogruppen und sonstige Ansteckungsverdächtige ausgeschöpft sind und sich als unzureichend erwiesen haben.

2.1.7. Berechtigungsscheine für kostenlose anonyme AIDS-Untersuchungen

Das Staatsministerium für Arbeit und Sozialordnung bat um datenschutzrechtliche Stellungnahme zu einer im Januar 1988 anlaufenden Aktion, in der Berechtigungsscheine für kostenlose HIV-Untersuchungen bei niedergelassenen Ärzten und in poliklinischen Einrichtungen der Hochschulen angeboten werden. Interessierte Bürger sollen bei den gesetzlichen Krankenkassen Berechtigungsscheine ohne Angaben ihrer Personalien abholen und dem Arzt ihrer Wahl vorlegen können. Der Arzt erfaßt vom Untersuchten lediglich Geschlecht, Alter in Jahren und die ersten beiden Ziffern der Postleitzahl des Wohnorts. Diese Angaben trägt er in einen Untersuchungsbogen in 4facher Ausfertigung ein. Blatt 1 verbleibt beim Arzt. Blatt 2 wird der Blutprobe beigefügt. Blatt 3 wird vom Labor ausgefüllt an den Arzt zurückgesandt. Blatt 4 wird zu Abrechnungszwecken vom Labor an die Kassenärztliche Vereinigung geschickt. Identifizierende Daten werden von keiner der beteiligten Stellen auf den Bogen vermerkt. In der Anweisung an die Ärzte wird auch darauf hingewiesen, daß die Abrechnung der Berechtigungsscheine für den HIV-Test getrennt von der Quartalsabrechnung der Kranken- und Überweisungsscheine erfolgen muß.

Der Landesbeauftragte für den Datenschutz ist der Auffassung, daß die oben genannten Angaben, die dem Umfang der Laborberichtspflicht weitgehend entsprechen, eine Identifizierung des Patienten nicht zulassen. Gegen das Verfahren bestehen keine datenschutzrechtlichen Bedenken.

2.2. Datenschutz im Krankenhaus

2.2.1. Datenerhebung bei der Krankenhausaufnahme

Aufgrund von Bürgereingaben hatte ich mich mit Formulierungen von Einverständniserklärungen bzw. Hinweisen zum Datenschutz in Krankenhausaufnahmeverträgen zu befassen. Die Überprüfung ergab, daß ein erheblicher Teil der

vorgesehenen Klauseln durch die Regelungen im neuen Art. 26 des Bayerischen Krankenhausgesetzes überflüssig geworden ist. Die Vorschrift gestattet dem Krankenhaus, ohne daß hierfür noch gesondert eine Einwilligung des Patienten einzuholen wäre, alle Daten zu erheben, zu speichern und zu nutzen, die zur Behandlung und zur verwaltungsmäßigen Abwicklung des Krankenhausaufenthalts erforderlich sind.

Art. 26 des Krankenhausgesetzes stellt klar, daß die personenbezogenen Patientendaten zur Aus-, Fort- oder Weiterbildung oder zu Forschungszwecken im Krankenhaus genutzt werden dürfen. Sie läßt auch die Auftragsdatenverarbeitung zu. Die Einholung der Einwilligung des Patienten ist insoweit nicht mehr erforderlich. Die Aufnahmeverträge können daher gestrafft werden. Ausdrückliche Einwilligungen sind allerdings immer noch erforderlich, soweit eine Datenverarbeitung über die nun gesetzlich zugelassenen Erhebungen, Speicherungen oder Nutzungen hinaus beabsichtigt ist, z. B. wenn eine Behörde, die sich mit der Erforschung von Straßenverkehrsunfällen befaßt, Einsicht in Patientendaten nehmen möchte, oder wenn Angaben für die Betreuung durch den Krankenhausseelsorger erhoben werden sollen.

2.2.2. Forschung mit Patientendaten im Krankenhaus

Ein Krankenhausträger hat angefragt, ob die nach Art. 26 Abs. 4 Satz 1 des Bayerischen Krankenhausgesetzes zulässige Nutzung von Patientendaten zu Forschungszwekken im Krankenhaus auch die Nutzung von Patientendaten durch einen anderen als den behandelnden Krankenhausarzt umfaßt.

Das Staatsministerium für Arbeit und Sozialordnung vertritt hierzu folgenden, nach meiner Auffassung richtigen Standpunkt: Bei einer Behandlung im Krankenhaus wechseln üblicherweise die behandelnden Ärzte. Ein Austausch der Patientendaten zwischen den einzelnen behandelnden Krankenhausärzten ist daher zwangsläufig. Er ist auch durch Art. 26 Abs. 4 Satz 1 (1. Alternative) BayKrG gedeckt. Daneben spricht die gesetzliche Regelung von einer möglichen Nutzung der Patientendaten, „soweit dies ... zur Aus-, Fort- oder Weiterbildung oder zu Forschungszwecken im Krankenhaus erforderlich ist". Daraus ist zu folgern, daß eine Nutzung von Patientendaten durch nicht behandelnde Krankenhausärzte zu den angegebenen Zwecken innerhalb des Krankenhauses auch ohne ausdrückliche Einwilligung des Patienten zulässig ist. Das Patienteninteresse bleibt auch gewahrt, wenn nicht behandelnde Krankenhausärzte die Patientendaten für die Forschung nutzen, da diese Ärzte ebenfalls der ärztlichen Schweigepflicht des § 203 StGB unterliegen.

2.2.3. Tumorzentrum München

Die datenschutzrechtliche Prüfung und Bewertung der Datenverarbeitung des Tumorzentrums München hat folgendes ergeben:

Das Tumorzentrum München ist ein Zusammenschluß von derzeit 42 Kliniken in Form eines Sekretariats innerhalb des Klinikums Großhadern. Die Datenverarbeitung wird durch das Universitätsinstitut für medizinische Informationsverarbeitung, Statistik und Biomathematik (ISB) abgewickelt. Die kooperierenden Kliniken übersenden auf Datenerfassungsbögen dem ISB die Daten behandelter Karzinom Patienten. Beim ISB werden die Daten, getrennt nach medizinischen und persönlichen Daten, in Dateien gespeichert.

Die Auswertung erfolgt zum Teil anonym statistisch, zum Teil „patientenorientiert". Für die patientenorientierte Nutzung erhalten die angeschlossenen Kliniken Listenausdrucke mit personenbezogenen medizinischen Daten ihrer Patienten. Während die statistische Aufbereitung in erster Linie Dispositionen der jeweiligen Klinik unterstützen soll, besteht der Zweck der patientenorientierten Aufbereitung vor allem in der Behandlung des einzelnen Patienten. Neben der rein therapeutischen Verwendung der Daten spielt jedoch auch hier die Auswertung zu wissenschaftlichen Zwecken eine Rolle, z. B. bei Promotionen oder Habilitationen.

Datenschutzrechtlich sind die gespeicherten Einzelangaben Patientendaten im Sinne des Art. 26 Abs. 1 Satz 1 des Bayerischen Krankenhausgesetzes (BayKrG). Nach meinen Feststellungen werden nur Daten erhoben und in die Tumordokumentation eingestellt, die zumindest auch Behandlungszwecken dienen. Eine Erhebung und Speicherung von Daten, die lediglich wissenschaftlichen Zwecken ohne Behandlungsbezug dienen, war nicht festzustellen. Werden für sonstige spezielle Untersuchungen besondere Daten benötigt, so wird hierfür eine zusätzliche schriftliche Einverständniserklärung eingeholt.

Ich habe gegen dieses Verfahren keine Bedenken erhoben. Die Speicherung der personenbezogenen Daten aus den im Tumorzentrum zusammengeschlossenen Kliniken beim ISB ist als Datenverarbeitung im Auftrag anzusehen. Verantwortlich im Sinne von Art. 26 BayKrG und daher auch Adressat der Rechte der betroffenen Patienten bleiben die auftraggebenden Kliniken. Sie sind für Auskünfte über gespeicherte Daten und die Bereinigung eventueller Fehler im Datenbestand zuständig. Zugriff auf die gespeicherten personenbezogenen Daten hat nur die jeweils auftraggebende Klinik. Da das ISB nach dem Organisationsbeschluß des Staatsministeriums für Unterricht und Kultus von 1974 eine klinische Einrichtung im Sinne des Art. 39 des Bayerischen Hochschulgesetzes ist, findet die Verarbeitung medizinischer Daten im Auftrag mithin „in einem Krankenhaus" im Sinne von Art. 26 Abs. 4 Satz 5 des Bayerischen Krankenhausgesetzes statt.

Fragen können sich noch bei der klinikübergreifenden Nutzung des Datenbestandes zu Forschungszwecken ergeben: Während innerhalb des Krankenhauses die Nutzung zu Forschungszwecken durch Art. 26 Abs. 4 Satz 1 und 2 ausdrücklich gestattet ist, ergibt sich aus der Vorschrift keine Lösung für die Frage, ob auch klinikübergreifende Nutzungen personenbezogener Patientendaten zu Forschungszwecken zulässig sind. Diese Frage bedarf noch der Klärung. Dabei wird zu berücksichtigen sein, daß der Patient in einem Universitätskrankenhaus mit Forschungs- und Lehrauftrag eher damit rechnet, daß seine Daten an andere Hochschulkliniken übermittelt werden, als wenn er sich in einem Krankenhaus einer niedrigeren Versorgungsstufe behandeln läßt.

2.2.4. Zentrale onkologische Dokumentation der Bayerischen Landesärztekammer und der Kassenärztlichen Vereinigung Bayerns

Der Landesbeauftragte für den Datenschutz hatte sich auf Bitte der Bayerischen Landesärztekammer und der Kassenärztlichen Vereinigung Bayerns (KVB) mit einem ADV-Ver-

fahren zu befassen, mit dem in einem Rechner bei der KVB Befunddaten über Krebspatienten erfaßt werden sollen.

Zusammen mit den Daten wird nur die laufende Nummer des Nachsorgekalenders eines Patienten, nicht aber dessen Name gespeichert. Behandelnde Ärzte und Kliniken sollen aufgrund einer ausdrücklichen und schriftlichen Einverständniserklärung des Patienten die Befunddaten auf einem mit der Nachsorgekalendernummer des behandelten Patienten versehenen Formblatt, dem Dokumentationsbogen, an die KVB senden. Zur Sicherstellung des Datenschutzes werden diese Dokumentationsbogen getrennt von den normalen Abrechnungsunterlagen versandt.

Der Patient entscheidet selbst, ob erstmals Daten an die zentrale Dokumentation übersandt werden. Gibt der Patient sein Einverständnis nicht, so erwachsen ihm für seine weitere Behandlung daraus keine nachteiligen Folgen. Er wird hierauf wie auch auf die Freiwilligkeit seiner Zustimmung ausdrücklich hingewiesen.

Muß sich der Patient zu einem späteren Zeitpunkt beispielsweise in einem anderen Krankenhaus oder von einem anderen Arzt behandeln lassen, entscheidet er jeweils neu durch die Vorlage des Nachsorge-Kalenders darüber, ob ein weiterer Arzt Daten der zentralen Dokumentation erhält und Daten dorthin übersenden darf. Die Daten des Patienten bleiben im Bereich der KVB anonymisiert und können nur durch Vorlage des Kalenders mit der entsprechenden Nummer beim behandelnden Arzt wieder einem bestimmten Patienten zugeordnet werden.

Die KVB hat darüber hinaus weitere Vorsorge für die Einhaltung der Datenschutzrechte getroffen. Sie verweist Auskunftsuchende zunächst an den behandelnden Arzt und stellt ihm für die Erteilung der Auskunft die erforderlichen Daten zur Verfügung. Wünscht der Patient jedoch die Erteilung der Auskunft unmittelbar durch die KVB, so wird auch dem entsprochen. Änderungswünsche des Patienten werden nach Möglichkeit im Benehmen mit dem behandelnden Arzt bearbeitet. Eine Sperrung von Daten ist nicht vorgesehen, nötigenfalls wird auf eine Speicherung gänzlich verzichtet bzw. werden beanstandete Daten gelöscht. Der Patient hat darüber hinaus das Recht, seine Zustimmung zur Speicherung der Daten jederzeit zurückzuziehen. In diesem Fall werden keine weiteren Daten über ihn gespeichert, bereits vorhandene Daten werden gelöscht.

Bedenken gegen das vorgesehene Verfahren haben sich nicht ergeben. Die Bereitschaft der Bayerischen Landesärztekammer und der Kassenärztlichen Vereinigung Bayerns, Anliegen des Datenschutzes zu berücksichtigen, möchte ich an dieser Stelle besonders hervorheben.

2.2.5. Datenerhebung für medizinische Forschung

In einer Eingabe wurde kritisiert, daß ein von einem medizinischen Hochschulinstitut an ältere Mitbürger gerichtetes Schreiben, in dem sie zur Teilnahme an einer wissenschaftlichen Befragung aufgefordert wurden, keinen eindeutigen Hinweis auf die Freiwilligkeit der Angaben enthalte. Das Schreiben sei geeignet, bei älteren Bürgern den Eindruck zu erwecken, daß sie die Befragung über sich ergehen lassen müßten.

Die Überprüfung ergab, daß das Institut für sein Forschungsvorhaben Namen und Anschrift von über 75 Jahre alten Personen aus dem Melderegister erhalten hatte. Eine solche Datenübermittlung ist zur rechtmäßigen Aufgabenerfüllung der Universität (hier wissenschaftliche Forschung) nach Art. 31 Abs. 1 des bayerischen Meldegesetzes grundsätzlich zulässig. Die Meldebehörde hatte im konkreten Fall die Übermittlung mit der Auflage verbunden, daß bei der Befragung der Personen ausdrücklich auf die Freiwilligkeit der Angaben hingewiesen werden müsse. Im Anschreiben an die Betroffenen war dies zwar nicht geschehen. Der an der Universität für die Befragungsaktion Verantwortliche hat aber die Interviewer angewiesen, vor der Befragung ausdrücklich auf die Freiwilligkeit der Angaben hinzuweisen. Gegen die nun gefundene Lösung habe ich keine Bedenken erhoben.

2.2.6. Datenerhebung für Forschungsprojekt „Rehabilitation von Krebskranken"

Ein privatrechtlich organisiertes Institut hatte vom Bundesministerium für Forschung und Technologie den Auftrag, im Rahmen eines Forschungsprojekts die Bedingungen zu untersuchen, unter denen Menschen, die von einer Krebserkrankung betroffen sind, in ländlichen Gebieten leben. Das Institut bat den Landesbeauftragten für den Datenschutz um Rat, wie es ohne Verstoß gegen Datenschutzrecht die Namen von Krebskranken, die sich im Krankenhaus befinden, erheben und die Kranken anschließend um Informationen bitten könne. Unter Mitwirkung meiner Geschäftsstelle wurde festgelegt, daß der Patient nach der Unterrichtung über das Vorhaben darüber entscheidet, ob der behandelnde Arzt dem Institut den Namen bekanntgibt und ein Mitarbeiter des Instituts einen Besuch am Krankenbett machen darf.

2.2.7. Weitergabe von Patientendaten an die European Dialysis and Transplant Association (EDTA)

In der Vergangenheit hatten bayerische Krankenhäuser – wie auch Krankenhäuser im übrigen Bundesgebiet – einen Patientenfragebogen mit detaillierten Angaben über namentlich genannte Dialyse-Patienten an die European Dialysis and Transplant Association (EDTA) in London übersandt. Nachdem sie darauf hingewiesen worden sind, daß hierzu die Einwilligungen der Betroffenen vorliegen oder diese Daten vorher anonymisiert werden müßten, haben nach Auskunft des Datenschutzbeauftragten des zuständigen Kuratoriums für Heimdialyse nahezu alle Dialyse-Patienten ihr Einverständnis zur Speicherung ihrer Dialysedaten bei der EDTA in London erklärt. Bis auf wenige Ausnahmen, die nicht mehr feststellbar waren, ist die Übermittlung und Speicherung damit rechtmäßig.

3. Sozialbehörden

3.1. Entwicklung von einwandfreien Antragsformularen

Bei örtlichen Prüfungen stelle ich immer wieder fest, daß die Sozialleistungsträger trotz gleicher Aufgabenstellung eine Vielzahl von unterschiedlichen Antragsformularen verwenden. Als Beispiele sind das Formular für Sozialhilfe bei den Sozialämtern und der Fragebogen für Adoptions- und Pflegekindverfahren bei den Jugendämtern zu nennen. Antragsformulare für Sozialhilfe unterscheiden sich nicht nur in ihrem äußerlichen Aufbau, sondern auch nach Umfang und Inhalt der Daten, die beim Antragsteller abgefragt werden, und im Inhalt der Einwilligungserklärungen, die bei dieser Gelegenheit vom Antragsteller gefordert werden.

Gleiches gilt für die genannten Fragebögen von Jugendämtern.

Bei der Überprüfung einzelner Fragebogen war festzustellen, daß es für manche Fragestellungen an der Rechtsgrundlage für eine Datenerhebung und die nachfolgende Datenspeicherung fehlt. So wurden beispielsweise Angaben über die Religionszugehörigkeit und über den schuldigen Teil einer Ehescheidung erfragt. In Adoptivverfahren waren z. B. Fragebogen über Persönlichkeit und körperliche Verfassung der leiblichen Eltern des Kindes vorgesehen. Häufig fehlte auch der Hinweis auf die Freiwilligkeit der Angaben, wie ihn § 9 Abs. 2 BDSG vorsieht, wenn es an einer Rechtsvorschrift für die Datenerhebung mangelt.

Meinen Hinweisen halten die Ämter häufig entgegen, sie würden die beanstandeten Formulare von privaten Verlagen beziehen und hätten deshalb auf die Gestaltung der einzelnen Fragen keinen Einfluß.

In den beiden genannten Beispielsfällen habe ich inzwischen bei der Konzipierung von Musterformularen unter Federführung der fachlich zuständigen Dienststellen (Landkreisverband, Landesjugendamt) mitgewirkt. Die neuen Musterentwürfe entsprechen meinen Vorstellungen.

3.2. Gemeinsame Stammdatenbankverwaltung von Sozial- und Jugendamt

Ein Landratsamt hat mich um Stellungnahme gebeten, ob die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) eine gemeinsame Stammdatenbankverwaltung für das Sozialamt und das Jugendamt aufbauen darf. Das Vorhaben wurde damit begründet, daß bestimmte personenbezogene Daten über Kinder und deren Eltern für alle Sachbearbeiter der beiden Ämter gleichermaßen zur Verfügung stehen müßten. Die Sachbearbeiter sollten mit Bildschirmgeräten auf den Datenbestand zugreifen können.

Gegen die gemeinsame Datenverwaltung mußte ich grundsätzliche datenschutzrechtliche Bedenken geltend machen. Ungeklärt war die für den Datenschutz wichtige Frage, welche Stelle (Sozialamt oder Jugendamt) oder beide oder eine Kombination aus beiden als speichernde Stelle im Sinne des § 2 Abs. 3 Nr. 1 Bundesdatenschutzgesetz (BDSG) bzw. Art. 5 Abs. 3 Nr. 1 BayDSG anzusehen ist. Diese Stelle trägt die Verantwortung für die Richtigkeit der gespeicherten Daten; gegen sie richten sich die Rechte des Betroffenen auf Auskunft, Berichtigung usw.

Die abfragende Stelle kann auf einen gemeinsamen Datenbestand von personenbezogenen Daten zugreifen, die sie nur zum Teil selbst erhoben hat. Das widerspricht aber der Regelung in § 69 Abs. 1 Nr. 1 SGB X über die Zulässigkeit der Offenbarung personenbezogener Daten zwischen dem Sozialamt und Jugendamt. Danach ist eine solche Offenbarung nur zulässig, soweit sie (im Einzelfall) zur Aufgabenerfüllung der jeweiligen Stelle erforderlich ist. Kann im Verfahren nicht sichergestellt werden, daß Zugriffe nur auf solche Daten möglich sind, die in eigener Zuständigkeit erhoben worden sind, oder an die andere Stelle weitergegeben werden dürfen, ist die gemeinsame Stammdatenbankverwaltung unzulässig.

3.3. Veröffentlichung von Sozialdaten in einem Leserbrief

Aufgrund einer Beschwerde hatte ich folgenden Sachverhalt zu untersuchen:

In einem Leserbrief, der in der örtlichen Tageszeitung veröffentlicht war, hat sich ein Bürger in allgemeinen Ausführungen über angebliche Mißstände bei der Gewährung von Sozialhilfe beklagt. Dazu nahm der zuständige Landrat in der Presse Stellung. Den Verfasser des Leserbriefes bezeichnete er dabei als arbeitslosen, arbeitsfähigen Sozialhilfeempfänger. Diese Angaben konnten dem Leserbrief nicht entnommen werden; sie stammten vielmehr aus den Unterlagen des Sozialamtes.

Der Landrat berief sich bei der Preisgabe der persönlichen Daten seines Kontrahenten auf die Notwendigkeit, die bestehenden Regelungen der Sozialhilfe als angemessen zu verteidigen.

Nach § 69 Abs. 1 Nr. 3 SGB X ist eine Offenbarung personenbezogener Daten nur zulässig, soweit sie erforderlich ist „für die Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen; die Offenbarung bedarf der vorherigen Genehmigung durch die zuständige oberste Landesbehörde".

Zwar gehört es zu den Rechten und ggf. sogar zu den Pflichten eines Behördenleiters, unwahren Tatsachenbehauptungen über die Verfahrensweise seiner Behörde in der Öffentlichkeit entgegenzutreten. Im vorliegenden Fall hatte der Leserbriefschreiber aber nicht behauptet, daß er persönlich vom Sozialamt falsch behandelt worden sei. Er hatte nur grundsätzliche Ausführungen über die Lebensverhältnisse von Sozialhilfeempfängern gemacht. Es war daher nicht erforderlich und deshalb auch nicht zulässig, die genannten Sozialdaten zu seiner Person an die Öffentlichkeit zu tragen. Im übrigen lag auch die vorherige Zustimmung des Staatsministeriums für Arbeit und Sozialordnung nicht vor. Damit waren die Voraussetzungen für eine Offenbarung nach § 69 Abs. 1 Nr. 3 SGB X nicht erfüllt. Ich habe die Verfahrensweise des Landrats daher beanstandet.

3.4. Übermittlung von Anschriften von Erblindeten an Vereine für Blindenhilfe

Aufgrund der Anfrage eines Landtagsabgeordneten hatte ich mich mit der Frage zu beschäftigen, unter welchen Bedingungen die Landesversicherungsanstalten als Leistungsträger nach dem Zivilblindengeldpflegegesetz Adressen von neu Erblindeten an Vereine der Blindenhilfe weitergeben dürfen.

Die Landesversicherungsanstalten sind nach Art. 4 Abs. 2 Zivilblindengeldpflegegesetz an die Vorschriften zur Wahrung des Sozialgeheimnisses gebunden. Eine gesetzliche Offenbarungsbefugnis nach den §§ 68 ff SGB X besteht in den oben angeführten Fällen nicht; vielmehr muß eine Einwilligung des Betroffenen eingeholt werden, bei der nicht der Eindruck entstehen darf, die Gewährung von Zivilblindenpflegegeld hänge von der Einwilligung ab. Die Landesversicherungsanstalten legen dem Betroffenen inzwischen eine Einwilligungserklärung vor, die den Anforderungen entspricht.

3.5. Anonymisierung von Daten der Mutterschaft

Zum 1. April 1986 hat der Bundesausschuß der Ärzte und Krankenkassen im Zusammenhang mit den neu gefaßten Mutterschaftsrichtlinien einen neuen Mutterpaß eingeführt.

Die Kassenärzte sind nach § 368 p RVO gehalten, die von den Bundesausschüssen beschlossenen Richtlinien zu beachten. In den Mutterpaß sollen die Ärzte die Daten über die Geburt und die Abschlußuntersuchung in der 6. bis 8. Woche nach der Entbindung in ein Epikrisenblatt aufnehmen und dort zusätzlich noch einige Angaben zum Schwangerschaftsverlauf eintragen. Ein Doppel dieses Epikrisenblatts soll der Arzt seiner Kassenärztlichen Vereinigung (KV) zu statistischen Auswertungen zusenden. Zwar wird auf dem für die Kassenärztliche Vereinigung bestimmten Vordruck Name und Anschrift der Mutter und des Kindes nicht eingetragen, doch sind die Meldungen nicht als anonymisiert anzusehen, solange das Doppel des Epikrisenblattes der Einzelabrechnung des Arztes mit den genauen Personalien der Mutter beizufügen ist. Demzufolge könnte die Kassenärztliche Vereinigung bei eingehenden Epikrisenblättern jederzeit feststellen, auf welche konkreten Personen sie sich beziehen. Hier war zu klären, ob bei der Datenanforderung durch die Kassenärztliche Vereinigung die ärztliche Schweigepflicht eingehalten wird.

Auf meine Anfrage hat mir die Kassenärztliche Vereinigung Bayerns erklärt, daß sie in einem Rundschreiben den bayerischen Kassen- und Vertragsärzten mitteilen wird, daß die Epikrisenblätter im Rahmen der Mutterschaftsvorsorge – getrennt von den Abrechnungen – gesammelt in einem verschlossenen Umschlag bei der Kassenärztlichen Vereinigung einzureichen sind. Dadurch wird eine Identifizierung der Betroffenen ausgeschlossen. Eine Zusammenführung von Daten aus der Mutterschaftsvorsorge mit anderen statistischen Erhebungen ist bei der Kassenärztlichen Vereinigung nicht vorgesehen.

3.6. Einschaltung einer Gemeinde in das Widerspruchsverfahren über einen Rentenbescheid

Ein Bürger hat sich bei mir darüber beschwert, daß eine Landesversicherungsanstalt in einem Widerspruchsverfahren über einen Rentenbescheid die Gemeinde eingeschaltet hat. Die kreisangehörige Gemeinde sollte den Widerspruchsführer über die Rechtslage aufklären, ihn von der Aussichtslosigkeit seines Widerspruchs überzeugen und auf eine Rücknahme des Widerspruchs hinwirken. Zu diesem Zweck wurden der Gemeinde Einzelheiten über das Widerspruchsverfahren mitgeteilt.

Es war die Frage zu klären, ob und in welchem Umfang im Rahmen der Amtshilfe nach § 4 Abs. 1 SGB X eine kreisangehörige Gemeinde in der geschilderten Weise eingeschaltet werden kann.

Nach § 93 SGB IV haben die Versicherungsämter in allen Angelegenheiten der Sozialversicherung Auskunft zu erteilen und die sonstigen ihnen durch Gesetz oder sonstiges Recht übertragenen Aufgaben wahrzunehmen. Die obersten Verwaltungsbehörden der Länder können einzelne Aufgaben der Versicherungsämter den Gemeinden übertragen.

Das Staatsministerium für Arbeit und Sozialordnung hat erklärt, daß die Einschaltung der kreisangehörigen Gemeinden in den genannten Fällen grundsätzlich nicht in Betracht kommt. Dem Versicherten werde auf diese Weise zwar der Weg zum Versicherungsträger erspart. Auch das Gespräch mit dem oftmals persönlich bekannten Gemeindebeamten könne durchaus für die Vermittlung der Rechtsansicht des Versicherungsträgers von Vorteil sein. Nach Meinung des Staatsministeriums für Arbeit und Sozialordnung darf jedoch nicht übersehen werden, daß Gemeindebeamte regelmäßig keine sozialversicherungsrechtliche Vorbildung besitzen und sich daher im wesentlichen auf die Wiedergabe der schriftlichen Information des Versicherungsträgers beschränken müssen. Ein Abweichen von der Formulierung berge die Gefahr von Fehlern, für die der Versicherungsträger im Zweifel einzustehen habe.

Die Offenbarung von Sozialdaten an die Gemeinde war im Beschwerdefall unzulässig. Die Landesversicherungsanstalt hat ihr Verfahren inzwischen geändert.

3.7. Mitteilungen der Gemeinde über Fremdenübernachtungen gegenüber der Landwirtschaftlichen Berufsgenossenschaft

Eine Gemeinde wurde von der örtlich zuständigen Landwirtschaftlichen Berufsgenossenschaft aufgefordert, alle ihr bekannten Fremdenübernachtungen in landwirtschaftlichen Anwesen mitzuteilen. Die Mitteilung sollte bei der Landwirtschaftlichen Berufsgenossenschaft zur Festsetzung der Beitragsleistungen dienen. Die Gemeinde hat mich um Stellungnahme gebeten, ob die Datenweitergabe zulässig sei.

Nach § 807 Abs. 1 RVO hat der Unternehmer der Berufsgenossenschaft über die Unternehmensverhältnisse Auskunft zu geben, soweit es für die Beitragsleistung in der (landwirtschaftlichen) Unfallversicherung von Bedeutung ist. Erteilt der Unternehmer die Auskunft nach § 807 RVO nicht rechtzeitig oder unvollständig, so hat die Gemeinde die fehlenden Unterlagen festzustellen (§ 808 Abs. 2 RVO).

Nach meiner Auffassung ist dem Wortlaut der genannten Bestimmungen zu entnehmen, daß die Mitwirkungspflicht der Gemeinde auf (benannte) Einzelfälle beschränkt ist. Eine Anforderung, über alle zimmervermietenden Landwirte im Gemeindegebiet Daten zu liefern, wäre demnach nicht zulässig.

Soweit Unterlagen über die Fremdenverkehrsabgabe für die Auskunft herangezogen werden, ist zu beachten, daß diese gemäß Art. 13 Abs. 1 Nr. 1 c Kommunalabgabengesetz (KAG) dem Steuergeheimnis (§ 30 AO) unterliegen. Nach § 31Abs. 2 der Abgabenordnung (AO) sind die Finanzbehörden jedoch berechtigt, die nach dem Steuergeheimnis geschützten Verhältnisse des Betroffenen den Trägern der gesetzlichen Sozialversicherung mitzuteilen. Das gilt auch für Verfahren zur Feststellung einer gesetzlichen Versicherungspflicht in Beitragsangelegenheiten.

Soweit landesrechtliche Vorschriften (z. B. das bayerische Meldegesetz) einer Datenübermittlung entgegenstehen, gehen die Bestimmungen der Reichsversicherungsordnung als Bundesrecht vor.

Ergänzend habe ich die Landwirtschaftliche Berufsgenossenschaft noch darauf hingewiesen, daß sie im Hinblick auf den Wortlaut des § 808 Abs. 2 RVO imstande sein muß, im Einzelfall – etwa bei einer Beschwerde – den Nachweis zu führen, daß der betreffende Unternehmer die Auskunft nach § 807 RVO nicht rechtzeitig oder unvollständig gegeben hat. Dies setzt voraus, daß ein entsprechender Fragebogen zunächst unmittelbar an den landwirtschaftlichen Unternehmer versandt worden ist.

3.8. Darf eine Sozialbehörde der Polizei das Erscheinen einer gesuchten Person mitteilen?

Mehrfach sind Sozialbehörden mit der Frage an mich herangetreten, ob eine Sozialbehörde die Polizei benachrichtigen darf, wenn diese darum für den Fall gebeten hatte, daß sich eine bestimmte Person in den Räumen der Sozialbehörde einfindet. Folge einer solchen Benachrichtigung wird in der Regel die Festnahme des Betroffenen sein. Ich habe diese Frage mit den zuständigen bayerischen Ministerien erörtert.

Das Staatsministerium des Innern hat im Einvernehmen mit dem Staatsministerium für Arbeit und Sozialordnung wie folgt Stellung genommen:

„Das Kammergericht Berlin hat in seinem Urteil vom 26.5.1983 den gegenwärtigen Aufenthalt einer Person (z. B. den Aufenthalt in einem Dienstgebäude) als Minus zur derzeitigen Anschrift im Sinne von § 68 Abs. 1 SGB X betrachtet und deshalb deren Offenbarung ebenfalls nach § 68 SGB X beurteilt. Ein anderer Sachverhalt liegt nach unserer Auffassung vor, wenn die Polizei eine Sozialbehörde für den künftigen Fall um Nachricht bittet, daß sich eine Person dort einfindet.

Die Befugnis zur Offenbarung der derzeitigen Anschrift bzw. des derzeitigen Aufenthalts nach § 68 Abs. 1 SGB X umfaßt unseres Erachtens nicht auch die Befugnis, Aufenthaltsanfragen zu speichern oder sonst zu vermerken und der Polizei künftige Aufenthalte des Betroffenen in der Sozialbehörde mitzuteilen. Diese Offenbarungen unterliegen daher nicht den erleichterten Voraussetzungen des § 68 SGB X."

Ich habe mich dieser Rechtsauffassung angeschlossen.

Vor einer Datenoffenbarung, die sich auf § 68 SGB X stützt, sind nach dieser Vorschrift die schutzwürdigen Belange des Betroffenen in Erwägung zu ziehen. Die Feststellung, ob eine Beeinträchtigung schutzwürdiger Belange vorliegt, erfordert eine Güterabwägung zwischen den Interessen des Betroffenen und dem öffentlichen Interesse an der Mitteilung seines Aufenthalts an die Polizei.

In Übereinstimmung mit den Staatsministerien des Innern und für Arbeit und Sozialordnung vertrete ich dazu die Auffassung, daß für die genannte Frage § 30 Abs. 4 Nr. 5 der Abgabenordnung (AO) insoweit eine Orientierungshilfe liefert, als in den dort aufgeführten Fällen (z. B. Verbrechen, schwere Vergehen, erhebliche Wirtschaftsstraftaten) stets davon auszugehen ist, daß das öffentliche Interesse überwiegt. In anderen Fällen ist zu berücksichtigen, daß die in § 68 SGB X aufgeführten Daten (Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift, derzeitiger Arbeitgeber) vom Gesetzgeber als weniger schutzwürdig angesehen wurden als andere bei einem Sozialleistungsträger gespeicherten Daten. Soweit die Daten für die Ermittlungen der Staatsanwaltschaft oder der Polizei im Rahmen eines Strafverfahrens benötigt werden, wird in der Regel das öffentliche Interesse an der Offenbarung gegenüber den Belangen des Betroffenen überwiegen. Bei der Prüfung der Zulässigkeit der Übermittlung von Daten im Rahmen von Ordnungswidrigkeitenverfahren ist die Schwere der jeweiligen Ordnungswidrigkeit zu berücksichtigen.

Dieser Beurteilung steht auch die Regelung in § 73 SGB X nicht entgegen. Nach dieser Vorschrift können zwar nur bei den dort besonders genannten Straftaten und auf richterliche Anordnung Sozialdaten offenbart werden. § 73 SGB X ermächtigt für die Aufklärung eines Verbrechens andererseits zur Offenbarung aller erforderlichen Sozialdaten, während § 68 SGB X nur zur Offenbarung bestimmter, wenig sensibler Daten berechtigt.

Bei verschiedenen Einrichtungen der Sozialbehörden – etwa bei der Familienhilfe – ist ergänzend zu prüfen, ob die Voraussetzungen sonstiger Schweigeverpflichtungen vorliegen.

Aus § 4 Abs. 3 Nr. 3 SGB X ergibt sich, daß eine ersuchte Sozialbehörde nicht verpflichtet ist, im Rahmen der Amtshilfe der Staatsanwaltschaft oder Polizei eine Auskunft zu erteilen, wenn sie unter Berücksichtigung der Aufgaben der ersuchenden Behörde durch die Hilfeleistung die Erfüllung ihrer eigenen Aufgaben ernstlich gefährden würde.

4. Polizei

4.1. Zur Lage des Datenschutzes

Dem Sicherheitsbereich und hierbei vor allem der Datenverarbeitung bei der Polizei ist in der Datenschutzdiskussion der letzten Jahre teilweise ein großer Stellenwert eingeräumt worden. Diese Diskussion hat mit dazu beigetragen, daß bei den Bürgern ungerechtfertigte Ängste gegenüber der Datenverarbeitung bei den Sicherheitsbehörden geweckt worden sind. Ich werde bestrebt sein, diese Diskussion ohne Vernachlässigung der Datenschutzbelange zu versachlichen.

Tatsächlich lautet das Resümee der Datenschutztätigkeit im Berichtszeitraum für den Polizeibereich, daß ernsthafte Datenschutzverstöße nicht festgestellt worden sind. Daß vereinzelt Fehler auftreten, liegt in der Komplexität der eingesetzten neuen Informationstechnik und in der nun einmal nicht fehlerfreien menschlichen Natur begründet. Sämtliche festgestellten Fehler beruhen indes nicht auf vorsätzlichen Datenschutzverstößen. Die bayerische Polizei verdient also auch bei der Datenverarbeitung das Vertrauen der Bürger.

Wenn die nachfolgenden Ausführungen länger als zunächst beabsichtigt geworden sind, dann mag dies auch als Beleg dafür dienen, daß der Polizeibereich nicht vernachlässigt wird.

4.2. Schwerpunkte meiner Tätigkeit

Wie in den vergangenen Jahren lagen die Schwerpunkte meiner Tätigkeit im polizeilichen Bereich bei generellen und auf Eingaben hin veranlaßten Prüfungen, bei der Beantwortung von zahlreichen Bürgereingaben und der Beratung der Sicherheitsbehörden.

Prüfungen

Neben den auf Grund von Eingaben notwendigen Kontrollen habe ich insbesondere bei folgenden Behörden Prüfungen vor Ort vorgenommen:

Landeskriminalamt
Präsidium der Bayerischen Grenzpolizei
Polizeidirektion Nürnberg

Polizeidirektion Traunstein
Polizeidirektion Rosenheim

Selbstverständlich konnten bei diesen Prüfungen nur Teilbereiche der Datenverarbeitung der geprüften Behörden herausgegriffen und durchgesehen werden. Die Prüfungen mußten sich zudem wie bisher im wesentlichen auf Stichproben beschränken.

Die Bürgereingaben in Polizeisachen nehmen nach wie vor einen erheblichen Teil meiner Arbeitskapazität in diesem Bereich in Anspruch. Die meisten in Eingaben geäußerten Befürchtungen von Bürgern, zu Unrecht in polizeilichen Dateien gespeichert zu sein, stellen sich bei meinen Nachprüfungen als unbegründet heraus. Soweit tatsächlich im Einzelfall Daten unzulässig gespeichert sind, löschen oder berichtigen die betroffenen Polizeibehörden die Daten auf meine Anregung hin umgehend. Die auf Bürgereingaben hin vorgenommenen Einzelfallprüfungen haben also wie schon in den Jahren zuvor in der überwiegenden Zahl der Fälle keine Verletzungen von Datenschutzbestimmungen ergeben.

Beratung

Ein Beweis für das zunehmend entspannte Verhältnis zwischen Polizei und Datenschutz und das meiner Geschäftsstelle entgegengebrachte Vertrauen sind die vielfältigen Anfragen der Polizeibehörden zur Anwendung von Datenschutzvorschriften im Einzelfall. Im Berichtszeitraum habe ich mich außerdem auf Anforderung des Staatsministeriums des Innern zu Automationsvorhaben sowie zu neuen Rechts- und Verwaltungsvorschriften im Sicherheitsbereich geäußert. Diese teilweise sehr arbeitsaufwendige und nach ihren Erfolgen nicht exakt meßbare Beratungstätigkeit ist der Versuch, möglichst bereits vorbeugend Datenschutz zu verwirklichen und nicht erst Konfliktfälle entstehen zu lassen.

4.3. Führung und Auswertung von kriminalpolizeilichen Sammlungen (KpS)

Die Speicherung in polizeilichen Dateien oder die Anlegung von Kriminalakten berührt das Persönlichkeitsrecht der Bürger in besonderem Maße. Der Bayerische Verfassungsgerichtshof (vgl. Entscheidung vom 9.7.1985, NJW 1986, S. 915) führt dies u. a. auf den Zweck polizeilicher Datensammlungen, ihren personenbezogenen Inhalt und das sich aus ihnen ergebende umfangreiche Persönlichkeitsbild zurück. Deshalb muß meines Erachtens bei der Speicherung personenbezogener Daten in polizeilichen Dateien und bei der Führung polizeilicher Akten sowie bei Datenübermittlungen aus solchen Sammlungen in besonderem Maße darauf geachtet werden, daß nur richtige, im Einzelfall erforderliche Daten in der jeweils zulässigen Zeitspanne gespeichert und nur den berechtigten Polizeibeamten zur Verfügung gestellt sowie nur im konkreten erforderlichen Einzelfall übermittelt werden. Diese Grundsätze habe ich wie in den vergangenen Jahren meinen Prüfungen zugrunde gelegt; auf die diesbezüglichen Ausführungen in früheren Tätigkeitsberichten nehme ich Bezug.

Aus der obengenannten Entscheidung des Bayer. Verfassungsgerichtshofes wird außerdem die Notwendigkeit einer bereichsspezifischen Regelung für die Führung personenbezogener kriminalpolizeilicher Sammlungen deutlich. Der Bayer. Verfassungsgerichtshof stellt nämlich ausdrücklich fest, daß es derzeit für die Führung von personenbezogenen kriminalpolizeilichen Sammlungen an der gebotenen gesetzlichen Regelung fehle. Zur Begründung erklärt das Gericht, daß die Ausführungen des Bundesverfassungsgerichts in der Entscheidung zum Volkszählungsgesetz 1983 (E 65, 1 ff) zum „Recht auf informationelle Selbstbestimmung" jedenfalls in ihren Grundaussagen auch zur Auslegung von Art. 100 und Art. 101 Bayer. Verfassung herangezogen werden könnten. So sei der Anspruch des Bürgers, daß die Voraussetzungen und der Umfang zulässiger Beschränkungen dieses Rechts gesetzlich festgelegt seien, für die Freiheit der Persönlichkeit von besonderer Bedeutung. Der derzeit im Polizeiaufgabengesetz enthaltenen polizeirechtlichen Generalklausel könnten Maßstäbe für Gegenstand, Ausmaß und Begrenzungen zulässiger Aktensammlungen für polizeiliche Zwecke nicht in der gebotenen Klarheit entnommen werden. Deshalb erscheine es nach Art. 101 i.V.m. Art. 100 Bayer. Verfassung geboten, daß der Gesetzgeber die Materie regelt, die bisher Gegenstand der Richtlinien für die kriminalpolizeilichen Sammlungen ist. Dabei müßten jedoch wegen der umfassenden Speicherung und Verwendung persönlicher Daten in den Kriminalakten im Gesetz selbst Abgrenzungen zwischen den Rechten des einzelnen einerseits und den Interessen der Allgemeinheit andererseits vorgenommen werden. Hierfür seien bestimmtere und eingehendere gesetzliche Regelungen geboten als sie in einer polizeirechtlichen Generalklausel gefunden werden könnte.

Allerdings weist der Bayer. Verfassungsgerichtshof darauf hin, daß solche Regelungslücken, wie sie derzeit im Polizeirecht bestehen, unter Umständen für eine gewisse Übergangszeit hingenommen werden könnten, um dem Gesetzgeber ausreichend Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zu lassen. Derzeit dürfte diese Übergangszeit wohl noch nicht abgelaufen sein. Nach meiner Auffassung muß jedoch der Gesetzgeber bis spätestens Ende der laufenden Legislaturperiode die notwendigen gesetzlichen Regelungen für die polizeiliche Datenverarbeitung schaffen. Zwar ist eine Abstimmung der Regelungen in einem Polizeigesetz mit den ebenfalls neu zu schaffenden Vorschriften in der Strafprozeßordnung zweifellos wünschenswert. Dies darf jedoch nicht zu einer ungebührlichen Verzögerung der Novellierung des Polizeirechts führen. Dabei ist zu berücksichtigen, daß bereits seit Frühjahr 1986 ein neuer „Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder" vorliegt, der für die Novellierung des Polizeiaufgabengesetzes eine grundsätzlich geeignete Grundlage darstellt. Auf die Ausführungen im 8. Tätigkeitsbericht, S. 24, weise ich hin.

4.3.1. Kriminalaktennachweis (KAN)

Zunächst erläutere ich einige Funktionsprinzipien des Kriminalaktennachweises (KAN) zum besseren Verständnis der nachfolgenden Ausführungen:

Der in Dateienform geführte KAN dient dem Nachweis von Kriminalakten, die bei den Ländern und beim Bund geführt werden. Er gliedert sich in einen Bundes-KAN, einen Landes-KAN und in den sog. regionalen KAN.

Der Bundes-KAN, der als Verbunddatei im polizeilichen Informationssystem INPOL Bund und Ländern zum Abruf zur Verfügung steht, soll sich darauf beschränken, Hinweise

zu geben auf Täter besonders schwerer katalogmäßig aufgelisteter Straftaten oder auf Täter von Straftaten mit überregionaler Bedeutung. Letzteres haben die eingebenden Polizeibeamten durch Vergabe entsprechender „KAN-Merker" zu entscheiden.

Im Landes-KAN und im regionalen KAN – eine bayerische Besonderheit – werden die Kriminalakten bayerischer Polizeidienststellen nachgewiesen. In dem bei den einzelnen Polizeidirektionen geführten regionalen KAN werden weitgehend dezentralisiert die Nachweise über Akten der Personen geführt, die lediglich auf örtlicher Polizeiebene von Bedeutung sind. Im Landes-KAN, der seinem Namen entsprechend auch landesweit abrufbar ist, werden die übrigen Nachweise zu den bayerischen Kriminalakten geführt. Aus datenschutzrechtlicher Sicht ist die in Bayern durchgeführte Trennung in Landes-KAN und regionalen KAN sehr zu begrüßen, weil sie den datenschutzrechtlichen Grundsatz berücksichtigt, daß Zugriff auf personenbezogene Daten nur die Stellen bekommen sollen, die diese Daten zu ihrer Aufgabenerfüllung benötigen. Bei weniger bedeutsamen Informationen sind dies im Regelfall nur die örtlichen Polizeibehörden.

Weil der KAN einen wesentlichen Überblick über die bei bayerischen Polizeidienststellen geführten Informationen erlaubt, habe ich wie in den Jahren zuvor auch im Berichtszeitraum dem KAN besonderes Augenmerk gewidmet. Neben einer allgemeinen Nachprüfung auf der Grundlage von Computerausdrucken bei 11 Polizeidirektionen habe ich noch zwei Polizeidirektionen vor Ort stichprobenartig kontrolliert.

KAN-Prüfungen

Die von 11 Polizeidirektionen erbetenen Listenausdrucke aus dem Kriminalaktennachweis betrafen

- Kinder
- Personen über 70 Jahre
- Ordnungswidrigkeiten
- KAN-Merker 5 (planmäßige und überörtliche Begehungsweise von Straftaten)
- sonstige polizeiliche Gefahrenabwehr
- Gesamtausdrucke zu bestimmten Buchstabengruppen und
- die vorgesehenen Aktenaussonderungen zu bestimmten Jahren.

Die Auswertung dieser Unterlagen sowie die stichprobenartige Prüfung vor Ort bei zwei Polizeidirektionen lassen folgende Schlüsse zu:

Die Qualität der polizeilichen Datenbestände – aus datenschutzrechtlicher Sicht gesehen – hat sich im Berichtszeitraum weiter deutlich verbessert. Die hierbei festzustellende Verringerung der Datenbestände hat, wie mir ausdrücklich versichert worden ist, zu keiner Beeinträchtigung der polizeilichen Arbeit geführt. Trotz dieser wirklich positiven Grundtendenz haben meine Prüfungen noch einzelne Fehler aufgezeigt. Auf die im folgenden angesprochenen Bereiche sollten die Polizeidirektionen deshalb nach wie vor ihr Augenmerk richten:

Kinder, alte Menschen und Ordnungswidrigkeiten

Die Abnahme der Speicherungen über Kinder, alte Menschen und Ordnungswidrigkeiten machen die folgenden Zahlen einer Polizeidirektion deutlich:

Dort ist der Bestand an Kindern gegenüber der vorjährigen Überprüfung von 138 auf 16 gesunken. Die Zahl der gespeicherten alten Menschen ist von 545 auf 34 reduziert worden und der Bestand an Speicherungen wegen Ordnungswidrigkeiten beträgt nun 17 statt 320 Fälle. Zwar gelten derartige Zahlen nicht für alle Polizeidirektionen. In einigen Fällen war die Zahl der alten Menschen und auch die Speicherung wegen Ordnungswidrigkeiten noch vergleichsweise hoch. Deutlich wird aber die Bereitschaft, die Datenbestände zu bereinigen und im Interesse auch der Effektivität der polizeilichen Arbeit unnötige Speicherungen zu vermeiden.

Teilweise sind Kinder noch länger als die in den entsprechenden Richtlinien vorgesehenen zwei Jahre gespeichert. Ich gehe davon aus, daß es sich hierbei um begründete Einzelfälle handelt, die aber in den entsprechenden Unterlagen zumindest kurz begründet sein sollten.

Bei den alten Menschen ist zu berücksichtigen, daß nach der Errichtungsanordnung eine Aufnahme von Tatverdächtigen über 70 Jahren in den KAN und in die Kriminalakten grundsätzlich nur nach strenger Prüfung zulässig ist. Stichproben haben allerdings ergeben, daß der somit geforderte strengere Maßstab bei der Datenspeicherung noch nicht durchgehend angelegt worden ist.

Selbst wenn alte Menschen nur im regionalen KAN gespeichert werden, muß in jedem Einzelfall geprüft werden, ob dies nach der Errichtungsanordnung tatsächlich zulässig ist. Teilweise sind alte Menschen im Landes-KAN gespeichert und damit landesweit abrufbar, obwohl sie nur einer geringfügigen Straftat verdächtig waren.

Die Speicherungsebenen im KAN

Die Vergabe der „KAN-Merker", die die Speicherung der Daten im Bundes-KAN veranlassen, entspricht nun weitgehend den entsprechenden Richtlinien. Allerdings habe ich auch hier noch einige Fehler festgestellt. So werden Kleindelikte wie Ladendiebstahl und Leistungserschleichung durch die Vergabe entsprechender KAN-Merker im Bundes-KAN gespeichert. Dies stellt für die Betroffenen eine unnötige Beeinträchtigung ihrer schutzwürdigen Belange dar und belastet außerdem die polizeilichen Informationssysteme mit irrelevanten Daten.

Auch werden gleichartige Delikte teilweise im regionalen KAN und teilweise im Landes-KAN gespeichert, ohne daß ein Grund für die unterschiedliche Sachbehandlung ersichtlich wäre. So sind z. B. im Landes-KAN kleinere Ladendiebstähle gespeichert, obwohl der regionale KAN der richtigere Speicherungsort gewesen wäre. Ein verstärkter Erfahrungsaustausch sollte hier zu einheitlicher Anwendung der Richtlinien in der Praxis beitragen.

Erfassungs- und Bewertungsfehler

Nach wie vor habe ich einzelne offenkundige Erfassungsfehler festgestellt, die durch eigene Überprüfungen der Polizeibehörden festgestellt und ausgemerzt werden sollten. Gravierender als offenkundige Erfassungsfehler, die als solche bei aufmerksamem Lesen auch für den abfragenden Polizeibeamten schnell erkennbar sein müßten, sind Unrichtigkeiten bei der Bewertung einer Straftat. Bewertungsfehler wirken sich insbesondere dann stark aus,

wenn eine Straftat durch eine unrichtige Bewertung als Verbrechen statt als Vergehen angesehen wird und somit im Bundes-KAN, also bundesweit abfragbar, gespeichert wird. Teilweise liegen diese fehlerhaften rechtlichen Bewertungen von Straftatbeständen auch darin begründet, daß die Staatsanwaltschaft nicht, wie nach Nr. 11 der Mitteilungen in Strafsachen vorgeschrieben, der Polizei über den Verfahrensausgang oder ihre abweichende Bewertung berichtet. So war mir aus einem Vorgang bekannt, daß die Staatsanwaltschaft einen Sachverhalt, der bei der Polizei noch als Verdacht des versuchten räuberischen Diebstahls (Verbrechen, also Speicherung im Bundes-KAN) gewertet worden ist, „lediglich" wegen Verdachts des Diebstahls (also lediglich Speicherung im Landes-KAN) verfolgt hat.

Fehler werden auch noch bei der sog. retrograden Erfassung (Erfassung zurückliegender Vorgänge) gemacht. So werden zum Teil Sachverhalte erstmals automatisiert gespeichert, die länger als 10 Jahre zurückliegen und gelöscht sein müßten oder bereits mehrere Jahre alte Ordnungswidrigkeiten betreffen.

Ein Fehler, der leicht vermeidbar sein müßte, ist die doppelte Speicherung des gleichen Sachverhaltes. Damit kann der unrichtige Eindruck entstehen, daß der Betroffene bereits mehrfach straffällig geworden sei.

Noch nicht abschließend gelöst scheint mir die Speicherung von Sachverhalten unter dem Schlüssel „sonstige polizeiliche Gefahrenabwehr" zu sein. Hier stellt sich in besonderem Maße die Frage der Erforderlichkeit einer derartigen Speicherung in Kriminalakten und demzufolge im KAN. Die Verwendung dieses Schlüssels darf nicht dazu führen, daß die Richtlinien für die Anlage von Kriminalakten umgangen werden. Bei der Speicherung unter „sonstige polizeiliche Gefahrenabwehr" ist die Frage der Erforderlichkeit für die künftige Erfüllung polizeilicher Aufgaben mit strengem Maßstab zu prüfen. Dies gilt insbesondere bei Personen, die bisher bei der Polizei noch nicht gespeichert waren. Nach meiner Auffassung müssen sich aus dem jeweiligen Vorgang selbst konkrete Anhaltspunkte dafür ergeben, daß der Betroffene auch künftig Anlaß zu polizeilichen Maßnahmen geben kann oder die vorhandenen Erkenntnisse für die künftige Aufgabenerfüllung erforderlich sein werden. Beispielsweise bei Erfassung eines betrunkenen Fußgängers, der lediglich eine Nacht in einer Ausnüchterungszelle verbringt, dürften diese Voraussetzungen nicht im Regelfall vorliegen. Die Aufnahme muß deshalb besonders begründet sein.

Auch dürfen Vorgänge, die bereits aus anderen Gründen im KAN gespeichert sind, nicht ein zweites Mal mit einer eigenen Notierung unter dem Schlüssel „sonstige polizeiliche Gefahrenabwehr" gespeichert werden. So ist beispielsweise die Vorführung zu einem Gerichtsarzt unter diesem Schlüssel gespeichert worden, obwohl das zugrundeliegende Strafverfahren bereits im KAN gespeichert war.

Meines Erachtens wird den Speicherungen unter dem Schlüssel „sonstige polizeiliche Gefahrenabwehr" von den vorgesetzten Dienststellen allein schon wegen der teilweise großen Zahl an Speicherungen (bei einer Direktion knapp 5 % sämtlicher Speicherungen) besonderes Augenmerk zu widmen sein. Derartige Speicherungen dürfen nicht zu einer Aufhebung der notwendigen strikten Trennung zwischen Kriminalaktenführung und Vorgangsverwaltung führen.

Inzwischen hat die Polizei nach meiner Prüfung erste Konsequenzen gezogen. So hat eine Polizeidirektion, die 922 Personen unter dem Schlüssel „polizeiliche Gefahrenabwehr" gespeichert hatte, inzwischen 181 Akten vollständig ausgesondert und aus 741 Kriminalakten mit Mehrfacheintragungen 705 Vorgänge gelöscht.

Manche Speicherungen wären vermeidbar, wenn die Polizei die von ihr selbst getroffene Bewertung eines Sachverhaltes als „unbedeutend" auch bei der Prüfung der Erforderlichkeit einer Speicherung berücksichtigen würde. So drohte z. B. ein Ehemann mit Selbstmord, falls seine Ehefrau nicht zu ihm zurückkehren würde. Aus der polizeilichen Akte geht eindeutig hervor, daß die Polizei selbst die Androhung des Selbstmordes nicht ernst genommen hat. Gleichwohl ist der Betroffene wegen Verdachts der versuchten Nötigung im Landes-KAN gespeichert. Hier wäre eine besondere Begründung für die Aufnahme angezeigt.

Speicherungsdauer

Bei der Vergabe von Wiedervorlagefristen, die zur Prüfung einer evtl. Aussonderung wesentlich sind, stelle ich mit Genugtuung fest, daß die Polizei hierbei zunehmend auf die Bedeutung des Falles abstellt. Zwar ist diese „Flexibilität" bei der Fristvergabe noch nicht bei allen Polizeidirektionen festzustellen, doch ist die grundsätzlich zu sehende Tendenz begrüßenswert. Allerdings finden sich bei der Fristvergabe vereinzelt noch offenkundige Fehler. So habe ich Fälle gefunden, in denen statt der Regelfrist von 10 Jahren ohne nähere Begründung Aussonderungsprüfdaten von 13 bis 15 Jahren festgesetzt worden sind. Auch für eine Ordnungswidrigkeit ist ein Aussonderungsprüfdatum von 10 Jahren grundsätzlich viel zu lang.

Ich bin überzeugt, daß die bestehende gute Zusammenarbeit mit den Dienststellen der Bayerischen Polizei dazu beitragen wird, die datenschutzrechtliche Qualität der Speicherungen im Kriminalaktennachweis noch weiter zu verbessern.

4.3.2. Polizeipräsidium München

Als Zusammenfassung meiner Prüfung beim Polizeipräsidium München hatte ich im 8. Tätigkeitsbericht den Eindruck wiedergegeben, „daß dem Datenschutz beim Polizeipräsidium München bislang noch nicht der notwendige Stellenwert eingeräumt worden ist". In der Zwischenzeit hat sich das Polizeipräsidium München umfassend mit meinen kritischen Feststellungen auseinandergesetzt und unternimmt offenbar derzeit alle Anstrengungen, die datenschutzrechtlichen Mängel zu beheben. Zwar tritt das Polizeipräsidium München in einigen Punkten (z. B. bei der Speicherung von kurzzeitig Vermißten) meinen Anregungen nicht bei. Doch handelt es sich hier nicht um zentrale Fragen.

Zwischenzeitlich sind auch wesentliche Voraussetzungen dafür geschaffen worden, die besonders gerügte Kriminalaktenführung zu verbessern. So wurde mit Weisung vom 1.12.1986 eine Trennung zwischen Vorgangsverwaltung und Kriminalaktenhaltung eingeführt. Diese aus der Sicht des Persönlichkeitsschutzes unabdingbare Trennung ist eine Vorbedingung dafür, daß künftig Daten von Beschuldigten und Verdächtigten nicht mit Daten von Zeugen, Anzeigenerstattern oder Hinweisgebern vermengt werden. Die zuletzt genannten Personen sind grundsätzlich nur in der sog. Vorgangsverwaltung und nicht personenbezogen suchbar in den Kriminalakten aufzunehmen.

Nach Auskunft des Polizeipräsidiums München hat sich der Bestand an Kriminalakten auf ca. 380.000 verringert. 140.000 Kriminalakten seien nicht älter als 5 Jahre. 1986 seien 280.000 Akten überprüft worden. Mit der vollständigen Überarbeitung der Akten sei im Laufe des Jahres 1988 zu rechnen. Diese ist im Hinblick auf die Datenerfassung für den Kriminalaktennachweis eine wesentliche Voraussetzung.

Die fehlende Abstimmung zwischen der Kriminalaktensammlung und der auf der Ebene der Dezernate und Kommissariate geführten Karteien hatte ich ebenfalls beanstandet, weil sie zur Folge hatte, daß trotz Aussonderung in der Kriminalaktensammlung in den anderen Karteien weiterhin Daten gespeichert geblieben sind, die für die Aufgabenerfüllung der Polizei nicht mehr erforderlich waren. Um die notwendige inhaltliche Übereinstimmung der einzelnen Karteien zu gewährleisten, hat das Polizeipräsidium nun die Weisung erteilt, daß die Dezernate und Kommissariate Karteien personenbezogen nur noch führen dürfen, wenn sich darüber in der Kriminalaktensammlung ein Hinweis befindet. Damit soll der für die Aussonderung und für eventuelle Auskünfte erforderliche Überblick über den Datenbestand gewährleistet werden.

Das Polizeipräsidium hat im übrigen auch seine Übersicht über die bei ihm geführten Dateien nach eigenen Angaben aktualisiert und vervollständigt.

Abgesehen von Kontrollen im Einzelfall und der Karteien im Zusammenhang mit der Homosexualität (siehe dort) habe ich im Berichtszeitraum keine Nachprüfung beim Polizeipräsidium München vorgenommen. Dies ist für das Jahr 1988 vorgesehen.

4.4. Prüfung beim Bayerischen Landeskriminalamt

Wie bereits frühere datenschutzrechtliche Prüfungen beim Landeskriminalamt hat auch die diesjährige Prüfung erwiesen, daß das Landeskriminalamt, dessen Effizienz allgemein anerkannt ist, dem Datenschutz den ihm gebührenden Stellenwert einräumt. Das belegt einmal mehr die Erfahrung, daß effektive polizeiliche Aufgabenerfüllung und richtig verstandener und praktizierter Datenschutz kein Widerspruch sind. Das Landeskriminalamt hat früh erkannt, daß der datenschutzrechtliche Grundsatz, wonach nur die Daten gespeichert werden dürfen, die zur gesetzlich zugewiesenen Aufgabenerfüllung tatsächlich erforderlich sind, letztlich mit dem Ziel einer wirkungsvollen polizeilichen Informationsverarbeitung weitgehend übereinstimmt. Zwar waren auch bei der diesjährigen datenschutzrechtlichen Prüfung beim Landeskriminalamt einige Fehler bei der Datenverarbeitung festzustellen. Doch waren diese Fehler nicht in organisatorischen Mängeln des Landeskriminalamtes, sondern in menschlicher Unvollkommenheit begründet, die nie ganz auszuschalten sein wird. Außerdem hat das Landeskriminalamt, das in nahezu allen Fällen die Bewertung des Datenschutzbeauftragten geteilt hat, die entsprechenden Daten umgehend berichtigt oder vernichtet.

Prüfungsansätze waren diesmal die automatisierte Kriminalaktenführung, die SPUDOK-Datei „Falschgeld", die Lage- und Tagesmeldungen sowie die Dateien APIS (Arbeitsdatei PIOS – Innere Sicherheit) und APOK (Arbeitsdatei PIOS – Organisierte Kriminalität). Zu den Ergebnissen der Prüfung bei den Lage- und Tagesmeldungen und der Datei APIS weise ich auf die diesbezüglichen gesonderten Ausführungen hin.

- Die automatisiert geführte **Kriminalaktenführung** stellt beim Landeskriminalamt kein Problem dar. Kleinere Fehler betrafen noch nicht ausgesonderte Vorgänge. So bestand noch eine Akte über den Streit zwischen Hausnachbarn, obwohl das Ermittlungsverfahren von der Staatsanwaltschaft mangels öffentlichen Interesses eingestellt war. In einem anderen Fall waren vor Jahren durchgeführte Anfragen anderer Polizeibehörden personenbezogen dokumentiert oder es fand sich eine unzulässig geführte Akte zu einem Kind. In einem Fall war im Kriminalaktennachweis zum gleichen Sachverhalt eine Doppelspeicherung vorgenommen worden. Das Landeskriminalamt hat diese Vorgänge zwischenzeitlich ausgesondert bzw. gelöscht. Es hat im übrigen auch zugesagt, die parallel neben dem Landes-KAN geführten eigenen Akten im Verlauf der ständigen Sachbearbeitung zu bereinigen.

- Die **SPUDOK-Datei „Falschgeld"** soll es der Polizei ermöglichen, den überörtlich auftretenden Straftäter in Falschgeldsachen zu ermitteln und zwischen Geschädigten, die selbst nur versehentlich eine Falschgeldnote erhalten haben, und den Personen zu unterscheiden, die vorsätzlich Falschgeld verbreiten. Die Datei wird seit Ende 1985 betrieben. Die kurze datenschutzrechtliche Prüfung der SPUDOK-Datei „Falschgeld" hat folgendes ergeben:

  Das Hauptproblem der SPUDOK-Datei „Falschgeld" – aber dies ist ein grundsätzliches Problem vieler SPUDOK-Dateien – dürfte die teilweise unterschiedliche Behandlung und Bewertung gleichgelagerter Sachverhalte einerseits in der SPUDOK-Datei „Falschgeld" und in der Datei Kriminalaktennachweis sein. Die Übereinstimmung der Aussonderungsprüffristen scheint ebenfalls nicht immer gewährleistet zu sein. So war ein Betroffener in der SPUDOK-Datei mit einer Wiedervorlagefrist von 3 Jahren und im Kriminalaktennachweis zum selben Sachverhalt mit einer Wiedervorlagefrist von 10 Jahren gespeichert.

  Das Datum zur Wiedervorlage für die Prüfung der Aussonderung wurde programmgesteuert in Abhängigkeit vom Eingabedatum, das mit der für die Fristberechnung maßgeblichen Tatzeit meist nicht übereinstimmt, in die Erfassungsbildschirme eingestellt. Dies hatte in einigen Fällen zur Folge, daß die Daten länger als erforderlich gespeichert geblieben wären. Aufgrund dieser Feststellung hat das Landeskriminalamt sofort das Programm geändert. Statt des Computers hat nun der Sachbearbeiter das Aussonderungsdatum zu vergeben.

  Die Richtigkeit der in Dateien nur in Kurzform gespeicherten Informationen muß nachprüfbar sein. In einzelnen Fällen war diese Nachprüfbarkeit bei der SPUDOK-Datei „Falschgeld" nicht ausreichend gegeben. Allerdings hat das Landeskriminalamt grundsätzlich Sorge dafür getragen, daß bei korrekter Sachbehandlung die Berechtigung der Speicherung und die Richtigkeit der Daten kontrolliert werden können.

Das Landeskriminalamt hat nach meiner Überprüfung den gesamten Datenbestand im Falschgeldbereich überarbeitet und festgestellte Mängel beseitigt.

- Die **Arbeitsdatei PIOS – Organisierte Kriminalität (APOK)** dient ihrem Titel entsprechend der Aufklärung von Straftaten, die der organisierten Kriminalität zuzurechnen sind. Die kurze Prüfung der Datei APOK hat keine datenschutzrechtlichen Besonderheiten ergeben. Die Datei ist derzeit noch nicht sehr umfangreich. Erfreulich war hier, daß die Richtigkeit der gespeicherten Daten auf Grund einer vorzüglichen Dokumentation leicht nachvollziehbar war. Die der Speicherung zugrundeliegenden Unterlagen werden übersichtlich in Aktenordnern geführt. Als datenschutzrechtlich korrekt habe ich auch festgestellt, daß Daten von geschädigten Personen oder solchen Betroffenen, die zufällig bei strafprozessualen Ermittlungshandlungen anwesend waren, weder in APOK noch im Kriminalaktennachweis gespeichert worden sind. Augenmerk wird bei dieser Datei darauf zu richten sein, daß die in der Datei vorgesehene Trennung zwischen Verdächtigen und Beschuldigten dem Sachstand der Ermittlungen entsprechend korrekt vorgenommen wird.

  Wie oben bemerkt finden sich Prüfungsergebnisse zu den „Lage und Tagesmeldungen" und zur Datei APIS in den jeweiligen Abschnitten des Tätigkeitsberichtes.

4.5. Personengebundene Hinweise

Die Diskussion um „personengebundene Hinweise" ist nicht zuletzt wegen der Speicherung von Hinweisen auf die HIV-Infektion in polizeilichen Informationssystemen erneut entfacht.

4.5.1. Entwicklung

Personengebundene Hinweise werden in polizeiliche Informationssysteme eingestellt. Sie beschreiben bestimmte Eigenschaften der gespeicherten Personen. Dies können Hinweise auf Prostitutionsausübung, Geisteskrankheit, Rauschgiftkonsum, Stadtstreicherei oder Bewaffnung sein, um einige dieser katalogmäßig aufgelisteten personengebundenen Hinweise zu nennen. Diese Hinweise sollen u. a. folgenden Zwecken dienen:

- Zur Eigensicherung des einschreitenden Beamten,
- zur Einleitung gezielter Fahndungsmaßnahmen,
- zur Unterstützung der polizeilichen Ermittlungen und
- zum Schutz des Betroffenen bei polizeilichen Maßnahmen.

Die personengebundenen Hinweise sollen der Polizei also eine erste Einschätzung der gespeicherten Personen erlauben.

An der Notwendigkeit einzelner personengebundener Hinweise insbesondere in Fahndungsdateien habe ich allein schon wegen der berechtigten Eigensicherung der einschreitenden Polizeibeamten nie Zweifel gelassen. So muß der Polizeibeamte, der einen ausgeschriebenen Straftäter festnehmen will, darüber unterrichtet sein, ob der Straftäter in früheren Fällen bewaffnet aufgetreten oder als gewalttätig bekannt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Befürchtung geäußert, daß die Speicherung derartiger Hinweise „die Gefahr der Ergreifung polizeilicher Maßnahmen nur auf Grund des Dateiinhalts hervorruft und daß sie ganz allgemein zu einer sozialen Abstempelung der betroffenen Person führen kann".

Ich teile diese Befürchtung nicht. Die Speicherung solcher Hinweise erleichtert der Polizei die Beurteilung der Lage, ohne aber die alleinige Entscheidungsgrundlage zu sein. Die Vermutung, ein personengebundener Hinweis in einem polizeilichen Informationssystem könne ganz allgemein zu einer sozialen Abstempelung führen, ist durch die Lebenserfahrung nicht belegt. Mit einer solchen Vermutung wird die Wirkung eines solchen Hinweises auf die soziale Umwelt des Betroffenen weit überschätzt. Wenn diese Hinweise für die polizeiliche Aufgabenerfüllung geeignet und dienlich sind und nicht außer Verhältnis zum angestrebten Zweck stehen, bestehen aus meiner Sicht gegen ihre Verwendung keine grundsätzlichen Bedenken. Bei der Aufnahme personengebundener Hinweise muß allerdings sichergestellt sein, daß sich die Richtigkeit dieser Hinweise aus Unterlagen belegen läßt und diese Daten regelmäßig auf ihre Aktualität überprüft werden.

Die auf Grund der Überlegungen der Datenschutzbeauftragten in den zuständigen Polizeigremien geführten Beratungen haben zur Streichung der personengebundenen Hinweise „geistesschwach", „entmündigt" und „internationaler Rechtsbrecher" geführt. Die weiteren Beratungen der zuständigen polizeilichen Arbeitsgruppe deuten darauf hin, daß der Katalog der personengebundenen Hinweise noch weiter verringert wird, die einzelnen Katalogbegriffe präziser definiert, diese nur für die tatsächlich relevanten Anwendungen verwendet werden und außerdem die Speicherungsdauer der einzelnen personengebundenen Hinweise der Bedeutung des einzelnen Hinweises angemessen und teilweise abhängig vom Alter des Betroffenen festgelegt wird. Durch die Begrenzung der Speicherungsdauer der einzelnen personengebundenen Hinweise soll verhindert werden, daß durch Zeitablauf möglicherweise unrichtig gewordene Hinweise (z. B. ein Hinweis auf die Ansteckungsgefahr durch eine schnell heilbare Krankheit) ungebührlich lange zum Nachteil des Betroffenen gespeichert bleiben.

4.5.2. Problem der Datenorganisation

Durch Prüfungen auf Grund einer Eingabe ist mir das nachstehende Problem der Nachweisschwierigkeiten über die Herkunft von personengebundenen Hinweisen deutlich geworden:

Das polizeiliche Informationssystem INPOL ist eine Verbunddatei, die von Bund und Ländern bedient wird. Dateneingaben, -löschungen und -abrufe können Dienststellen des Bundes und der Länder vornehmen. Auch können Daten, die von einer oder mehreren Dienststellen in das INPOL-System eingegeben sind, von anderen Dienststellen um weitere Informationen ergänzt werden. Grundsätzlich kann die Dienststelle, die Daten eingibt, diese auch wieder löschen.

Gehört zu den Daten, die von einer anderen Dienststelle hinzugespeichert werden, ein personengebundener Hinweis, kann folgendes Problem auftreten: Der personengebundene Hinweis wird programmgesteuert zu dem von den weiteren Informationen getrennten Personaldatensatz hinzugespeichert und bleibt dort stehen, auch wenn die übrigen hinzugespeicherten Daten später gelöscht werden. Das hat zur Folge, daß es sich in der Regel nicht mehr feststellen läßt, wer diesen personengebundenen Hinweis

gespeichert hat. Die Dienststelle, deren Daten einschließlich des von einer anderen Dienststelle eingefügten personengebundenen Hinweises weiter gespeichert bleiben, besitzt über Herkunft und Grund der Speicherung des personengebundenen Hinweises keine Unterlagen. Dies führt dazu, daß die Verantwortung für die Vergabe des personengebundenen Hinweises und dessen Richtigkeit nicht mehr nachvollziehbar sind. Damit sind aber Erforderlichkeit und Richtigkeit dieser Hinweise nicht in allen Fällen gewährleistet.

Hier muß meines Erachtens eine Lösung gefunden werden, die sicherstellt, daß die für die Vergabe des personengebundenen Hinweises verantwortliche Dienststelle erkennbar bleibt und dort auch die Zulässigkeit des Hinweises durch die Führung ausreichender Unterlagen überprüfbar ist.

4.5.3. Speicherung von HIV-Infektionen im polizeilichen Informationssystem

Im polizeilichen Informationssystem INPOL sowie in der Datei Kriminalaktennachweis wird für HIV-Infizierte, die bereits in kriminalpolizeilichen Sammlungen gespeichert sind oder nach denen gefahndet wird, der personengebundene Hinweis „ANST" (Ansteckungsgefahr) mit dem Zusatz „Vorsicht, Blutkontakte" vergeben. Grundlage für diese Speicherung ist der Beschluß der Arbeitsgemeinschaft der Leiter der Landeskriminalämter und des Bundeskriminalamts, wonach bei Personen, die in Verdacht stehen, bzw. bei denen es erwiesen ist, daß sie die Immunschwächekrankheit AIDS übertragen können, zu Eigensicherungszwecken für Polizeibeamte auf diese Gefahr hinzuweisen ist. Die Innenministerkonferenz hat diese Verfahrensweise zur Kenntnis genommen. Auch sie vertritt die Meinung, daß aus Gründen der Fürsorge für Polizeibeamte, die mit Infizierten in Kontakt kommen können, in bestimmten Fällen eine Speicherung der AIDS-Infizierung erfolgen muß, dies dürfe aber aus datenschutzrechtlichen Gründen nur im erforderlichen Umfang geschehen. Die Innenministerkonferenz hat deshalb den Auftrag erteilt, unter Beteiligung der Datenschutzbeauftragten entsprechende Kriterien für die Speicherung zu erarbeiten und ihr zur Beschlußfassung vorzulegen.

Derzeit ist bundesweit zu ca. 350 Personen ein entsprechender Hinweis gespeichert. Für Bayern lautet die vergleichbare Zahl 35 (Stand Oktober 1987). Meine zu den bayerischen Speicherungen durchgeführten Ermittlungen haben ergeben, daß in der überwiegenden Zahl der Fälle der Betroffene selbst der Polizei die Tatsache der HIV-Infektion mitgeteilt hat. In einigen Fällen rühren die Erkenntnisse von Justizvollzugsanstalten her. Ganz überwiegend sind von der Speicherung männliche und weibliche Prostituierte sowie vor allem Rauschmittel-Konsumenten betroffen.

Besonders hervorzuheben ist, daß mit der Vergabe des personengebundenen Hinweises keine polizeiliche „AIDS-Datei" eingerichtet wird. Der Hinweis ist nicht abrufbar. Vielmehr erhält den Hinweis auf AIDS nur derjenige Polizeibeamte, der in den kriminalpolizeilichen Sammlungen oder in der Fahndungsdatei einen bestimmten Namen abruft.

Der Bayerische Datenschutzbeauftragte vertritt bezüglich der Speicherung des personengebundenen Hinweises „ANST" mit dem Zusatz „Vorsicht, Blutkontakt" in polizeilichen Informationssystemen folgende Position:

Eine Speicherung dieses personengebundenen Hinweises ist datenschutzrechtlich zulässig, wenn folgende Voraussetzungen erfüllt sind:

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

Die Speicherung des personengebundenen Hinweises „ANST" mit dem Zusatz „Vorsicht, Blutkontakt" stellt zwar einen Eingriff in die Rechte der Betroffenen dar, ist aber unter den vorgenannten Voraussetzungen zum besseren Schutz der Polizeibeamten sowie im Einzelfall zum Schutze Dritter (z. B. Festnahme mehrerer Personen) erforderlich und geeignet sowie in Anbetracht des tödlichen Ausgangs einer HIV-Infektion auch verhältnismäßig.

Zwar sind bislang nur äußerst wenige Fälle einer HIV-Infizierung bei Polizeibeamten in Ausübung der dienstlichen Tätigkeit bekannt geworden. Doch stimme ich mit dem Staatsministerium des Innern darin überein, daß für die Polizei aus Erfahrungs- und Vernunftsgründen die Frage der nachgewiesenen Häufigkeit der Gefährdung unerheblich sein muß. Die Führung der Polizei hat nach Auffassung des Staatsministeriums des Innern aus Gründen der Fürsorge die Gefahr so weit wie möglich zu minimieren. Es zählten nicht die im Polizeidienst bisher erfolgten konkreten Ansteckungen, sondern das Bemühen, es möglichst zu keiner einzigen Ansteckung kommen zu lassen. Dieser Auffassung schließe ich mich an. Das erhöhte Infektionsrisiko für Polizeibeamte wird auch von medizinischer Seite gesehen. Hiernach kann der Kontakt mit dem Blut eines Infizierten die Infektion auch ohne Verletzung übertragen. Es reichen sogar kleinste, fast immer vorhandene Haut- und Schleimhautverletzungen als Eintrittspforte des Virus in den Körper aus. Bei dem derzeitigen Erkenntnisstand müsse angenommen werden, daß jeder Kontakt eines Polizeibeamten mit dem Blut eines Infizierten, auch ohne Verletzung des Beamten, zu einer Infektion führen könne.

Weil die Polizei nicht nur bei der Festnahme von in Fahndungsdateien ausgeschriebenen HIV-Infizierten in Körper- und Blutkontakt treten kann, sondern auch im Rahmen der sonstigen polizeilichen Tätigkeit Situationen vorstellbar sind – etwa bei Durchsuchungen oder erkennungsdienstlicher Behandlung –, in denen Polizeibeamte durch Infizierte verletzt und angesteckt werden können, ist eine Beschränkung des entsprechenden Hinweises auf Fahndungsdateien unzureichend. Vielmehr ist zum Schutz der Polizeibeamten und Dritter die Speicherung des Hinweises auch im Kriminalaktennachweis erforderlich. Bei den dort gespeicherten Personen wird auch in Zukunft regelmäßig davon auszugehen sein, daß Anhaltspunkte für die eventuelle Begehung künftiger Straftaten und somit für Kontakte mit Polizeibeamten vorliegen.

Auch die Beschränkung auf solche Infizierte, die als Gewalttäter bekannt sind, wird den Risiken polizeilicher Tätigkeit nicht gerecht. Nach polizeilichen Erkenntnissen werden auch bislang nicht als gewalttätig bekannte Bürger der Polizei gegenüber in manchen Ausnahmesituationen, z. B. bei einer Zwangsvorführung, handgreiflich.

Allerdings wird eine Speicherung des personengebundenen Hinweises dann nicht erforderlich sein, wenn die Polizei im konkreten Einzelfall davon ausgehen kann, daß der Betroffene entweder nicht mehr „polizeilich" in Erscheinung treten oder auf Grund seiner Persönlichkeitsstruktur kein Infektionsrisiko darstellen wird (z. B. infizierte Bluter).

Um allerdings zu vermeiden, daß bei Personen der Hinweis auf eine AIDS-Infektion gespeichert wird, die tatsächlich nicht infiziert sind, muß die HIV-Infektion ärztlich nachgewiesen sein. Aus vermeintlichen Krankheitssymptomen eines Betroffenen darf die Polizei keine zur Speicherung führenden Rückschlüsse ziehen. Selbstverständlich braucht das entsprechende ärztliche Attest der Polizei nicht unmittelbar vorzuliegen. Vielmehr genügt es, wenn die amtliche Stelle oder die Person z. B. ein Arzt, sich bei der entsprechenden Mitteilung an die Polizei ausdrücklich und glaubwürdig auf ein ärztliches Attest bezieht.

Teilt der Betroffene selbst der Polizei die HIV-Infektion mit, wird er auf die Speicherung in polizeilichen Dateien hinzuweisen sein, um ihm die Möglichkeit einer Berichtigung einer unzutreffenden Selbstbezichtigung einzuräumen. Dies gilt insbesondere dann, wenn Angehörige den Hinweis auf die AIDS-Infektion geben und hierbei nicht ausdrücklich das ärztliche Attest vorweisen können.

Das Staatsministerium des Innern hat meinen diesbezüglichen Überlegungen durch eine kürzlich erlassene Weisung entsprochen, wonach der Betroffene auf die Freiwilligkeit seiner Angaben hinzuweisen ist und zum Zwecke des Nachweises seiner Angaben eine schriftliche Bestätigung zu erfolgen hat. Bei einer Überprüfung im Landeskriminalamt, das den Hinweis auf die HIV-Infektion zentral für die bayerischen Polizeibehörden speichert, habe ich im übrigen eine einwandfreie Dokumentation zum Nachweis der Speicherungen vorgefunden.

Soweit andere Behörden der Polizei von einer HIV-Infektion Mitteilung machen, muß der Polizei gegenüber deutlich werden, daß diese Mitteilung auf einem entsprechenden ärztlichen Attest beruht. Ferner muß die Übermittlung rechtlich zulässig sein. Im einzelnen verweise ich auf die Ausführungen im Abschnitt „AIDS".

Während der ganzen Dauer der Speicherung eines personengebundenen Hinweises auf eine HIV-Inektion muß erkennbar sein, welche Dienststelle den Hinweis gespeichert hat und die zugrundeliegenden Unterlagen über Herkunft und Grund der Speicherung verwahrt. Dies ist wie auch in sonstigen Fällen die Voraussetzung dafür, daß die Verantwortung für die Vergabe des Hinweises und dessen Richtigkeit nachprüfbar sind und ggf. eine Berichtigung vorgenommen werden kann.

Soweit dies derzeit in einigen Fällen nicht möglich ist, sind möglichst kurzfristig die notwendigen organisatorischen oder programmtechnischen Maßnahmen zu treffen (vgl. auch 2.1.1 d am Ende).

4.6. Neuordnung der polizeilichen Meldewege

Die sog. „polizeilichen Meldedienste" sollen der (Verbesserung der) Information der einzelnen Polizeidienststellen, dem Erkennen überörtlicher Täter und der Aufklärung von Straftaten dienen sowie zum rechtzeitigen Handeln in Gefährdungssituationen und zur Konzentrierung polizeilicher Tätigkeit führen. Auf die generelle Bedeutung der Meldedienste und die mit ihnen verbundenen datenschutzrechtlichen Fragen bin ich in den vorangegangenen Tätigkeitsberichten eingegangen.

Zu diesen Meldediensten gehören auch die sog. **„Lage- oder Tagesmeldungen"**, mit denen nach bestimmten festgelegten Verteilern Meldungen im eigenen oder in den angrenzenden Präsidialbereich, an das Landeskriminalamt und auch an andere Bundesländer gegeben werden. Auf Grund meiner bereits im 7. Tätigkeitsbericht geäußerten Zweifel, ob der Inhalt dieser Meldungen tatsächlich einen sinnvollen Beitrag zur Effizienz polizeilicher Tätigkeit erbringen könne, hatte das Staatsministerium des Innern zunächst die Einstellung dieser Meldungen veranlaßt. Da die Einstellung offensichtlich eine Informationslücke hinterlassen hat, hat das Staatsministerium des Innern die Wiederaufnahme der „Lage- und Tagesmeldungen" angeordnet.

Den mit den „Lage- und Tagesmeldungen" erzeugten Informationsfluß sowie die Umsetzung dieser Informationen in personenbezogene Speicherungen beim Landeskriminalamt habe ich erneut überprüft: Die beim Landeskriminalamt durchgeführte Auswertung der Lage- und Tagesmeldungen erfolgt in einer aus datenschutzrechtlicher Sicht nicht zu beanstandenden Art und Weise. Aus diesen Meldungen werden tatsächlich nur die Sachverhalte gespeichert, die auch tatsächlich meldepflichtig und für das Landeskriminalamt zu seiner gesetzlichen Aufgabenerfüllung erforderlich sind. Allerdings hat sich bei dieser Prüfung wiederum gezeigt, daß mit diesen Meldungen von den nachgeordneten Polizeidienststellen auch solche Informationen an einen sehr großen Verteilerkreis gesteuert werden, die erkennbar für dessen Aufgabenerfüllung nicht erforderlich sind. So werden auch Vorfälle an andere Dienststellen gemeldet, die offensichtlich nur einen örtlich auftretenden Täter betreffen (z. B. Diebstahl einer alten Frau im Supermarkt). Weitere überregional gesteuerte Sachverhalte, die zur Aufgabenerfüllung nicht erforderlich sind, waren beispielsweise:

> Der versehentlich gelegte Zimmerbrand; das Randalieren im betrunkenen Zustand zu Hause und das Verbringen in die Ausnüchterungszelle; ein Suizidversuch; Trunkenheitsfahrt mit MOFA 25 ohne Sicherstellung eines Führerscheines; Blutentnahme nach Trunkenheitsfahrten; der Diebstahl von einigen Ster Brennholz; ein Ladendiebstahl von Gegenständen im Wert von 6,99 DM u. a. mehr.

Am Beispiel der Lage- und Tagesmeldungen kann ich nur die Mängel eines einzelnen Meldedienstes aufzeigen. Nach meiner Ansicht liegen die Probleme bei den regelmäßigen Datenübermittlungen zwischen den einzelnen Polizeibehörden u. a. darin begründet, daß eine Fülle von Datenübermittlungspflichten durch zahlreiche, teils parallele, teils sich überschneidende Meldedienste bestehen. Das hat in einzelnen Fällen nicht nur zur Folge, daß gleiche Sachverhalte mehrfach und z. T. auch mehrfach an den gleichen Empfängerkreis übermittelt werden müssen.

Neben dieser nicht unerheblichen Belastung für die Polizeidienststellen kann dies auch zu dem datenschutzrechtlich unerfreulichen Ergebnis führen, daß gleiche Sachverhalte – ohne daß dies sofort erkennbar ist – mehrfach in polizeilichen Dateien oder Karteien gespeichert werden. Die Überwachung der Richtigkeit solcher mehrfach gespeicherter Informationen, eine gleichmäßige Berichtigung und eine aufeinander abgestimmte Aussonderung ist unter diesen Umständen häufig nur schwer möglich. Ich möchte deshalb anregen, das polizeiliche Meldesystem mit den eingeführten Meldewegen auf seine Effizienz zu überprüfen und entbehrliche Meldewege einzustellen.

4.7. Arbeitsdatei PIOS – Innere Sicherheit (APIS)

Bereits in den beiden vorangegangenen Tätigkeitsberichten hatte ich mich mit der Datei APIS und im Zusammenhang damit mit dem Meldedienst Staatsschutz (KPMD-S) befaßt. Im Berichtszeitraum habe ich die Datei APIS beim Landeskriminalamt geprüft.

Die Datei APIS ist eine Verbunddatei des Bundes und der Länder. Sie dient der Verhütung und Aufklärung von Straftaten, soweit der Verdacht besteht, daß mit den Straftaten Ziele verfolgt werden, die insbesondere gegen die freiheitlich demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Hierzu sind in der Datei APIS Daten aufzunehmen, die zum einen, katalogmäßig aufgezählt, sog. politische Straftaten betreffen (u. a. §§ 80 ff, 102 ff StGB – Friedensverrat und weitere sog. „Staatsschutzdelikte"). Daneben werden Daten zu „anderen Straftaten" gespeichert, sofern wegen der Angriffsrichtung, des Motivs des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, daß die vorgenannten Ziele verfolgt werden.

Die Datei APIS wird beim Bundeskriminalamt geführt, die Dateneingabe erfolgt jedoch grundsätzlich vom und in Verantwortung des jeweiligen Landeskriminalamts, in dessen Zuständigkeitsbereich derartige Straftaten begangen werden. Grundlage und Anstoß für derartige Speicherungen in der Datei APIS sind die durch den entsprechenden polizeilichen Meldedienst für den Staatsschutz (KPMD-S) beim Landeskriminalamt eingehenden Informationen.

Beim Prüfungsergebnis sind zwei Bereiche zu unterscheiden: Die in der unmittelbaren Verantwortung des Landeskriminalamtes stehende Datenverarbeitung und die sich aus der engen Verzahnung von KPMD-S und APIS ergebenden datenschutzrechtlichen Fragen.

Das Landeskriminalamt ist sich bei der Führung der Datei APIS der besonderen Sensibilität der gespeicherten Daten und damit der Folgen etwaiger Fehler bei der Datenverarbeitung für die Betroffenen bewußt: Herkunft und Grundlage der in dieser Datei gespeicherten Daten können schnell und einwandfrei über gut organisierte Akten und Unterlagen nachgeprüft werden. Offensichtlich wird auch die Dateneingabe mit besonderer Sorgfalt vorgenommen; jedenfalls haben die Überprüfungen keine offenkundigen Erfassungsfehler erbracht. Schließlich nutzt das Landeskriminalamt für die Schulung neuer Mitarbeiter und für die Weiterbildung eine APIS-Testdatei. Etwaige „Lernfehler" haben somit keine Auswirkungen auf bereits erfaßte Originaldatensätze. Das Landeskriminalamt überprüft in erfreulich kurzen Zeitabständen, nämlich monatlich, inwieweit Datensätze der Datei zu löschen sind. Um die Aktualität und die Vollständigkeit der Daten zu gewährleisten, bemüht sich das Landeskriminalamt zudem – zumindest in Einzelfällen –, auch den jeweiligen Verfahrensausgang zu erfahren. Die Datei APIS bietet eigene Felder an, in die der jeweilige Verfahrensstand und der Verfahrensausgang gespeichert werden können.

Gerügt habe ich, daß in den dem Landeskriminalamt übermittelten Meldungen, die dann Grundlagen für eine Speicherung in APIS geworden sind, die persönliche Eigenschaft des Betroffenen – Beschuldigter, Verdächtiger, andere Person, Geschädigter – nicht vermerkt war, weshalb es dem Landeskriminalamt oblag, den Betroffenen „richtig" in die Datei einzuspeichern. Das Landeskriminalamt hat hierzu erklärt, daß es sich bei diesen Fällen um Fehler aus der Anfangsphase der Datei APIS handeln müsse. Später seien derartige Fehler nicht mehr vorgekommen.

Aufgefallen ist auch, daß Betroffene, die wegen des gleichen Sachverhalts sowohl in der Datei APIS wie in der Datei Kriminalaktennachweis gespeichert sind, mit unterschiedlichen Aussonderungsfristen in den beiden Dateien festgehalten sind. Dies ist zum Teil auf Grund der unterschiedlichen Regelungen in den einzelnen Errichtungsanordnungen für diese Dateien begründet, liegt zum anderen aber auch an einer nicht abgestimmten Sachbehandlung. Auf dieses Problem müssen die polizeilichen Sachbearbeiter hingewiesen werden, damit sie gleiche Sachverhalte möglichst gleich speichern lassen.

Mit dem Staatsministerium des Innern habe ich die Ergebnisse der APIS-Prüfung eingehend erörtert und in der Bewertung der festgestellten Sachverhalte weitgehende Übereinstimmung erzielt.

4.8. Weitere Einzelfragen

4.8.1. Personenkarteien strafbarer Homosexualität

Die Ausführungen im 8. Tätigkeitsbericht zu diesen Karteien haben zu besonders zahlreichen Eingaben geführt. Ich bin nicht nur den Einzelfragen nachgegangen, sondern habe mich nach der diesbezüglichen Praxis bei den übrigen bayerischen Polizeidienststellen erkundigt und sämtliche derartige mir bekanntgewordenen Karteien durchgesehen.

Die bisherige „Homo-Kartei" des Polizeipräsidiums München trägt nun die Bezeichnung „Personenkartei strafbarer Homosexualität und männliche Prostitution". Diese Kartei ist, wie stichprobenartige Überprüfungen ergeben haben, mittlerweile vollständig überarbeitet und deutlich verkleinert worden. Nach ihrer Errichtungsanordnung enthält sie nunmehr nur noch Beschuldigte und einer Straftat Verdächtigte (insbesondere Sittlichkeitsdelikte nach dem 13. Abschnitt des Strafgesetzbuches) oder Betroffene entsprechender Ordnungswidrigkeiten. Erfassungskriterium ist somit nicht die sexuelle Eigenschaft des Straftäters, sondern die von ihm begangene Straftat oder Ordnungswidrigkeit. Durch diese an der Tat orientierte Erfassung wird nicht der „Homosexuelle" allein wegen seiner sexuellen Veranlagung gespeichert, sondern, wie auch in anderen Karteien zu bestimmten Straftatengruppen, ausschließlich der einer Straftat Verdächtigte oder der Straftäter. Meine Stichproben haben die Beschränkung der Kartei auf diesen Personenkreis bestätigt gefunden. Auch Einzelüberprüfungen, die ich auf Grund von Eingaben vorgenommen habe, haben ergeben, daß nur die vorgenannten Personen

gespeichert werden und Personen, die im Rahmen einer Razzia in einer bestimmten Lokalität oder an sonstigen Treffpunkten Homosexueller kontrolliert worden sind, in dieser Kartei nicht enthalten sind.

Soweit bei einigen wenigen anderen Polizeistellen in Bayern vergleichbare Karteien geführt werden, haben meine Prüfungen ebenfalls zu keinen Beanstandungen geführt. Datenschutzrechtlich ist gegen die Führung solcher Karteien keine Einwendung zu erheben, wenn sie an den vorgenannten Kriterien orientiert sind. Sie sind zur wirksamen Verfolgung der mit Homosexualität zusammenhängenden Straftaten und der Folgekriminalität erforderlich.

4.8.2. Übermittlung von Sozialdaten an die Polizei

Sozialdaten sind durch das Sozialgeheimnis (§ 35 SGB I) besonders geschützt. Ihre Übermittlung an die Polizei ist nur in den gesetzlich besonders geregelten Fällen (§§ 68 ff SGB X) oder mit Einwilligung des Betroffenen zulässig.

Weil manche Bürger ihren sich aus dem Melderecht ergebenden Pflichten zur An- bzw. Abmeldung nicht nachkommen, sind ihre aktuellen Anschriften häufig nur über öffentliche Krankenkassen zu erlangen, denen aus einem Beschäftigungsverhältnis des Betroffenen die Wohnanschrift und der jeweilige Arbeitgeber bekannt sind. Nach § 68 SGB X kann der Polizei Name, Geburtsdaten, Anschrift sowie Name und Anschrift des derzeitigen Arbeitgebers übermittelt werden, soweit im Einzelfall kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Im Berichtszeitraum habe ich die datenschutzrechtliche Zulässigkeit der Anfragen von einigen Dienststellen des Polizeipräsidiums München beim Sozialreferat der Landeshauptstadt München geprüft. Hierbei hat sich in keinem Fall gegenüber den Polizeibehörden ein Anlaß zur Beanstandung ergeben. § 68 SGB X ist beachtet worden: Alle Anfragen beim Sozialreferat der Landeshauptstadt München nach Anschriften von Betroffenen und deren Arbeitgebern waren zur polizeilichen Aufgabenerfüllung erforderlich und sind erst erfolgt, nachdem aus anderen Quellen die erforderlichen Auskünfte nicht zu erhalten waren. Besonders erfreulich habe ich es gefunden, daß in allen geprüften Fällen die Polizeibeamten den Ablauf ihrer Nachforschungen und Anfragen bei anderen Behörden dokumentiert hatten.

Eine Prüfung bei der Polizeidirektion Nürnberg/Fürth hinsichtlich deren Anfragen nach § 68 SGB X beim Sozialreferat der Stadt Nürnberg hatte das gleiche positive Ergebnis. Bei keiner Stichprobe ist eine Verletzung des § 68 SGB X festgestellt worden.

Zur Abrundung sei in diesem Zusammenhang auf folgendes hingewiesen:

Ein Teil der von der Polizei durchzuführenden Aufenthaltsermittlungen, die dann im Gefolge auch Anfragen nach der Anschrift des Betroffenen bei Sozialleistungsträgern erforderlich machen, sind auf Aufenthaltsermittlungen zurückzuführen, die die Polizei auf Bitten anderer Behörden durchführt. Um die Polizei durch derartige Amtshilfeersuchen anderer Behörden nicht zu sehr zu belasten – allein im Zuständigkeitsbereich des Polizeipräsidiums München werden jährlich ca. 4000 derartige Amtshilfeersuchen gestellt – hat das Staatsministerium des Innern die ausdrückliche Weisung erteilt, die Beantwortung entsprechender Ersuchen künftig einzustellen. Die Behörden haben zunächst selbst zu versuchen, mit den ihnen zustehenden rechtlichen Mitteln (z.B. nach § 68 SGB X) den Aufenthalt von Betroffenen festzustellen. Dies ist auch aus datenschutzrechtlicher Sicht eine begrüßenswerte Maßnahme, da damit die Zahl der Datenübermittlungen von Sozialdaten an die Polizei deutlich verringert wird.

4.9. Bayerische Grenzpolizei

4.9.1. Personenkontrollen

Auch in diesem Berichtszeitraum haben sich wieder zahlreiche Bürger mit Fragen zur datenschutzrechtlichen Zulässigkeit einzelner im Rahmen der Grenzkontrolle durchgeführter Maßnahmen erkundigt. Immer wieder wird die Befürchtung geäußert, daß bei der Grenzkontrolle die Tatsache des Grenzübergangs auf Computern der Polizei gespeichert werde. Ich kann nur nochmals feststellen, daß diese Befürchtung grundlos ist.

Wie bereits in früheren Berichten festgestellt, bestehen für die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs eindeutige Rechtsgrundlagen: §§ 1 und 2 Bundesgrenzschutzgesetz, die auch für die Bayerische Grenzpolizei anwendbar sind. Im Rahmen dieser Kontrolle ist auch eine fahndungsmäßige Überprüfung einzelner Bürger zulässig. Hierzu kann es im Einzelfall erforderlich sein, daß sich die Polizeibeamten die fahndungsrelevanten Daten – in der Regel sind dies die Personalien – für die Abfrage in den polizeilichen Informationssystemen kurz notieren oder über ein Lesegerät in den entsprechenden Abfrageraum übermitteln lassen. Eine Speicherung auf diese Weise erhobener Personalien findet grundsätzlich nicht statt. Es werden keine Bewegungsbilder über Grenzübertritte erstellt. Vielmehr haben meine Ermittlungen in allen Fällen ergeben, daß Notizen mit Personalien nach der Fahndungsabfrage stets vernichtet worden sind.

Ein Bürger hat sich in diesem Zusammenhang darüber beschwert, daß ihm bei der Grenzkontrolle von dem kontrollierenden Beamten eine frühere Verurteilung vorgehalten worden sei und daß sein Reisebegleiter hiervon Kenntnis erlangt habe. Er äußerte die Befürchtung, die Grenzpolizei frage im Rahmen der Grenzkontrolle beim Bundeszentralregister an oder halte abgeschlossene Gerichtsverfahren Bürgern beim Grenzübertritt ohne berechtigten Anlaß vor.

Meine Ermittlungen hatten in diesem Falle ergeben, daß bei der fahndungsmäßigen Überprüfung die Ausschreibung des Betroffenen zur Strafvollstreckung wegen Unterschlagung festgestellt worden ist. Der kontrollierende Beamte hat dem Betroffenen zu Recht den Inhalt der fahndungsmäßigen Ausschreibung eröffnet. Der Mitreisende des Betroffenen hat sich wohl in dessen Nähe befunden und konnte das Gespräch mithören. Datenschutzrechtlich waren die Ausschreibung im polizeilichen Fahndungssystem und die Abfrage im Rahmen der Grenzkontrolle nicht zu beanstanden. Die Aufenthaltsermittlung war von der zuständigen Staatsanwaltschaft nach den für die Strafvollstreckung geltenden Vorschriften der Strafprozeßordnung veranlaßt worden.

Zur Frage des möglichen Mithörens eines Reisebegleiters ist festzustellen, daß darin keine Datenübermittlung im Sinne des Datenschutzrechts liegt, wenn der Begleiter nur aus

Versehen des Polizeibeamten von der Fahndungsausschreibung Kenntnis erhält. Allerdings sind im vorliegenden Fall die notwendigen organisatorischen Vorkehrungen gegen eine unbeabsichtigte Weitergabe von personenbezogenen Daten an Außenstehende nicht beachtet worden (Art. 15 BayDSG). Das Präsidium der Grenzpolizei hat mir hierzu mitgeteilt, daß der betroffene Beamte eingehend belehrt worden ist, künftig entsprechende Maßnahmen zu treffen, damit derartige ungewollte Datenweitergaben nicht mehr stattfinden.

4.9.2. Prüfung des Präsidiums der Bayerischen Grenzpolizei

Die beim Präsidium der Bayerischen Grenzpolizei geführten Dateien mit personenbezogenen Daten waren Gegenstand einer stichprobenartigen datenschutzrechtlichen Prüfung. Ernsthafte Verletzungen datenschutzrechtlicher Bestimmungen haben sich hierbei nicht ergeben.

Vielmehr hat sich gezeigt, daß seit meiner vorangegangenen Prüfung im Jahr 1983 die Datensammlungen erfolgreich bereinigt worden sind. So enthält die Zentralkartei statt ursprünglich 40.000 Karteikarten nunmehr nur noch 20.000 Karten.

Ein Augenmerk ist jedoch auf die Vergabe der Fristen für Wiedervorlage und Aussonderung von Vorgängen zu legen. Hier habe ich in einigen Fällen eine Überschreitung der Fristen festgestellt, ohne daß diese im jeweiligen Einzelfall sachlich veranlaßt gewesen wären. Das Präsidium der Grenzpolizei hat mir zugesichert, die Wiedervorlagefristen künftig noch flexibler, also am Einzelfall orientiert zu vergeben und das Aussonderungsprüfdatum jeweils sichtbar auf den einzelnen Vorgang anzubringen, um eine sachgerechte Aussonderung sicherzustellen.

Auch wird noch stärker als bisher darauf geachtet werden müssen, daß Karteikarten und zugehöriger Vorgang inhaltlich übereinstimmen. So haben Stichproben folgendes ergeben: In der Zentralkartei hat zum Beispiel noch eine Karte über einen Vorgang vorgelegen, obwohl dieser bereits vernichtet war. Umgekehrt ist trotz Aussonderung der diesbezüglichen Karteikarte der dazugehörige Vorgang weiter aufbewahrt worden, der infolge fehlender Karteikarte nicht mehr auffindbar gewesen ist.

Besonderen Wert lege ich grundsätzlich darauf, Doppelspeicherungen – also die doppelte Führung von gleichen Daten in verschiedenen Datensammlungen – zu vermeiden. Eine Doppelspeicherung ist in der Regel datenschutzrechtlich problematisch, weil häufig der gegenseitige Abgleich der einzelnen Datensammlungen nicht vollständig gewährleistet ist und somit zum gleichen Sachverhalt unterschiedliche Daten vorliegen können.

Bei meiner Prüfung habe ich solche Doppelspeicherungen personenbezogener Daten festgestellt, die aus dem grenzüberschreitenden Verkehr anfallen. Diese Daten werden sowohl beim Präsidium der Bayerischen Grenzpolizei wie bei den nachgeordneten Dienststellen geführt. Dieses Problem ist jedoch bereits erkannt und wird wohl durch die Einführung eines automatisierten Grenzaktennachweises gelöst werden. Ich werde die Einführung dieses Grenzaktennachweises beobachten.

5. Verfassungsschutz

5.1. Prüfungen beim Bayerischen Landesamt für Verfassungsschutz

Wie in den vorangegangenen Jahren hat sich meine Prüftätigkeit beim Bayerischen Landesamt für Verfassungsschutz auf die zur Beantwortung von Bürgereingaben notwendigen Kontrollen und eine kurze generelle Prüfung beschränkt. Hierzu kann ich als erfreuliches Ergebnis mitteilen, daß sich im Berichtszeitraum bei keiner einzigen der auf Grund von Bürgereingaben durchgeführten Kontrollen ein Anlaß zu einer datenschutzrechtlichen Beanstandung des Landesamtes für Verfassungsschutz ergeben hat. Das Landesamt für Verfassungsschutz hat mir im übrigen in allen Eingabefällen seine Unterlagen vorgelegt.

Diese Kontrollmöglichkeit des Landesbeauftragten bei Verfassungsschutzbehörden ist ein wichtiges, verfassungsrechtlich gebotenes Korrektiv dafür, daß den Bürgern in der Regel über eventuell bei Verfassungsschutzbehörden gespeicherte Daten aus Sicherheitsgründen keine Auskunft erteilt werden kann. Kontrollen durch eine unabhängige, weisungsfreie Institution sind geeignet, eventuelles Mißtrauen gegenüber Verfassungsschutzbehörden abzubauen und das Vertrauen in den demokratischen Rechtsstaat zu stärken.

Durch die Kontrolle des Datenschutzbeauftragten soll und darf das Landesamt für Verfassungsschutz nicht in der Erfüllung seiner Aufgabe behindert werden, Extremisten und Verfassungsfeinde zu beobachten und zu überwachen. Der Datenschutzbeauftragte ist nicht für Leute da, die den Verfassungsschutz diffamieren und abschaffen wollen, um ihre Ziele ungestörter verfolgen zu können.

Neben der Prüfung, ob sich der Verfassungsschutz bei der Erhebung und Verarbeitung von Daten im Rahmen seines gesetzlichen Auftrags bewegt und die gesetzlichen Schranken einhält, sehe ich meine Aufgabe in diesem Bereich vornehmlich darin, den durch unglückliche Umstände oder wegen einer Personenverwechslung versehentlich beim Landesamt für Verfassungsschutz gespeicherten unbescholtenen Bürger vor Nachteilen zu bewahren. Letztlich sehe ich mich in diesem Bemühen auch durch das ureigenste Interesse des Landesamts für Verfassungsschutz unterstützt.

Im Berichtszeitraum habe ich, wie oben bemerkt, das Landesamt für Verfassungsschutz wiederum zu einer kurzen generellen Prüfung aufgesucht. Schwerpunkte waren Feststellungen zur Rechtmäßigkeit und Richtigkeit der Speicherungen in NADIS (Nachrichtendienstliches Informationssystem) sowie der Informationsfluß an das Landesamt für Verfassungsschutz. Nähere Ansatzpunkte für die Prüfung waren dabei Datenspeicherungen im Zusammenhang mit Bürgerinitiativen und besonderen Einsatzschwerpunkten der Sicherheitsbehörden, Datenspeicherungen im Zusammenhang mit der Unterwanderung von Steuerhilfebüros durch extremistische Parteien, etwaige Auswertungen von Wahlunterstützungslisten sowie einige konkret benannte Personen, die aus anderen Anlässen bekanntgeworden waren. Außerdem habe ich darauf geachtet, daß die Richtigkeit der Daten nachgewiesen ist und die Daten nur über den für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz erforderlichen Zeitraum gespeichert werden.

Als Ergebnis kann ich meine Feststellung vom letzten Jahr wiederholen, daß sich das Bayer. Landesamt für Verfassungsschutz bemüht, die Anregungen des Datenschutzbeauftragten bei der Datenverarbeitung zu berücksichtigen.

Zur Frage der Speicherung der Teilnehmer von Veranstaltungen und der Mitglieder von Bürgerinitiativen hat das Landesamt für Verfassungsschutz ausdrücklich erklärt, daß Erhebung und Speicherung personenbezogener Daten in diesen Fällen ausschließlich am Einzelfall und streng am gesetzlichen Auftrag orientiert erfolgten. Soweit das Landesamt für Verfassungsschutz bei dort gespeicherten Personen auch die bloße Tatsache der Teilnahme an Veranstaltungen festhält, ohne daß im konkreten Einzelfall der Betroffene in einer für die Tätigkeit des Landesamts relevanten Weise auftritt, hatte ich ursprünglich datenschutzrechtliche Bedenken geltend gemacht. Dabei hatte ich auf die Ausführung des Bundesverfassungsgerichts (E 65, S. 1/43 ff) hingewiesen: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Das Staatsministerium des Innern hat demgegenüber jedoch überzeugend dargelegt, daß aufgabeneröffnend und -verpflichtend die ernsthaft verfolgte verfassungsfeindliche Zielsetzung ist, ohne daß es auf die konkreten Formen ankäme, in denen sie verfolgt werden mag. Verfassungsfeindliche Zielsetzungen würden regelmäßig im Rahmen der Ausübung von Grundrechten verfolgt. Der Beobachtung durch das Landesamt für Verfassungsschutz stünden auch nicht die vorgenannten Äußerungen des Bundesverfassungsgerichts entgegen, weil das Gericht ausdrücklich festgestellt habe, daß das „Recht auf informationelle Selbstbestimmung" und der damit verbundene grundsätzliche Schutz einer Grundrechtsausübung vor behördlicher Registrierung nicht schrankenlos sei. Der Einzelne müsse aus seiner Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit Einschränkungen seines „Rechts auf informationelle Selbstbestimmung" im überwiegenden Allgemeininteresse hinnehmen. Im übrigen enthalte das Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz die erforderliche Rechtsgrundlage, aus der sich die Voraussetzungen und der Umfang der Einschränkung des „Rechts auf informationelle Selbstbestimmung" eindeutig ergäben. Die Ausübung des Grundrechts und die Beobachtung durch die Verfassungsschutzbehörde schlössen sich somit nicht gegenseitig aus.

Im Hinblick auf diese Ausführungen des Staatsministeriums des Innern stelle ich meine früher geäußerten Bedenken zurück. Die Prüfung hat, legt man diesen von mir für richtig gehaltenen Maßstab an, keinen Anlaß zu Beanstandungen ergeben.

Die Prüfung hat außerdem gezeigt, daß die Sorgen mancher Bürger, Wahlunterstützungslisten würden vom Bayer. Landesamt für Verfassungsschutz generell ausgewertet und die darin erfaßten Personen in Dateien gespeichert, unbegründet sind. Die diesbezüglichen Erklärungen des Landesamts für Verfassungsschutz hat eine Stichprobe bestätigt. Auch hinsichtlich der Aufklärung einer eventuellen Unterwanderung von Steuerhilfebüros durch extremistische Parteien waren keine unzulässigen Datenspeicherungen beim Landesamt festzustellen.

Im übrigen haben sich während der Prüfung lediglich geringfügige Mängel in Einzelfällen gezeigt, die wohl trotz aller Bemühungen niemals völlig auszuschließen sein werden. Bei aller Schwierigkeit für den Datenschutzbeauftragten, die datenschutzrechtliche Richtigkeit von gespeicherten Informationen zu bewerten, da hierzu, wie mehrfach vermerkt, häufig die spezielle Fachkenntnis der Verfassungsschutzbehörden nötig ist, habe ich das Landesamt für Verfassungsschutz dennoch gebeten, dafür Sorge zu tragen, daß aus Gründen der Kontrollierbarkeit und auch aus Gründen der innerbehördlichen Nachvollziehbarkeit der Richtigkeit von Informationen Eintragungen in Dateien und Karteien innerhalb des Hauses präzise belegbar sind. Aus den Unterlagen muß deutlich werden, woher die einzelne Information stammt, welches Maß an vermuteter Richtigkeit ihr beizumessen ist und – in Zweifelsfällen – warum die Speicherung für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz erforderlich ist. Zu den Daten, die nachvollziehbar sein sollten, gehören auch die Zeitangaben, von denen ab üblicherweise die Aussonderungsfrist zu laufen beginnt.

Ein Anliegen, das ich gegenüber allen Behörden, nicht nur gegenüber dem Verfassungsschutz verfolge, ist die möglichst auf den Einzelfall abgestimmte Vergabe von Aussonderungsfristen. In der Mehrzahl der Fälle mögen die vorgesehenen „Regelaussonderungsfristen" der richtige Wert für eine Aussonderung sein. Hierfür sprechen auch Gründe der Einheitlichkeit der Sachbehandlung innerhalb einer Behörde. Soweit jedoch Vorgänge offensichtlich von der Norm abweichen, etwa weil der Verdacht einer verfassungsfeindlichen Betätigung besonders vage ist oder stärkere Zweifel an der Richtigkeit einer von außen eingelaufenen Information bestehen, rege ich die Vergabe von kürzeren Aussonderungsfristen an. Durch eine damit ermöglichte frühere Prüfung von Vorgängen – also vor Ablauf der üblichen Aussonderungsfristen – kann festgestellt werden, ob ursprünglich angenommene Verdachtsmomente noch bestehen oder inzwischen ausgeräumt sind. Auch kann gerade in solchen Fällen nochmals geprüft werden, ob auf Grund neuerer Erkenntnisse überhaupt noch ein örtlicher Bezug zum Bayerischen Landesamt für Verfassungsschutz besteht, oder ob die Abgabe an eine andere Behörde sachgerecht wäre.

Das Staatsministerium des Innern hat ausdrücklich versichert, daß bei der Bemessung von Wiedervorlagefristen Ermessensentscheidungen der mit der Materie vertrauten Sachbearbeiter trotz der detailliert geregelten Wiedervorlagefristen weiterhin möglich sein müssen, um formalistischen Schematismus zu vermeiden. Dies begrüße ich.

In diesem Zusammenhang möchte ich es ausdrücklich als erfreulich bezeichnen, daß ich beispielsweise in einem Vorgang feststellen konnte, daß die Vergabe eines von der Regelfrist abweichenden Wiedervorlagedatums ausdrücklich begründet worden ist. Eine solche Verfahrensweise entspricht meinen Anregungen. Daß im übrigen verkürzte Wiedervorlagefristen notwendig und sachgerecht sein

können, haben auch einzelne Fälle ergeben, in denen als Ergebnis meiner Prüfung entweder die Vorgänge vernichtet oder aber an zuständige Behörden abgegeben worden sind.

5.2. Sicherheitsüberprüfungen in der Privatwirtschaft zum Zwecke des Sabotageschutzes

Wie die Anschläge in der letzten Zeit auf Rechenzentren oder Einrichtungen der Elektrizitätswirtschaft zeigen, sind zahlreiche Betriebe der Privatwirtschaft von Sabotageakten bedroht. Um nach Möglichkeit zu verhindern, daß sabotagebereite Mitarbeiter in derart gefährdete Betriebe eingestellt oder innerhalb eines Betriebes in entsprechend gefährdete Bereiche umgesetzt werden, werden in der Privatwirtschaft Sicherheitsüberprüfungen durchgeführt. An diesen Sicherheitsüberprüfungen wirkt das Landesamt für Verfassungsschutz mit. Der Schutz anschlaggefährdeter Betriebe liegt im besonderen öffentlichen Interesse. Er ist kein bloßes Anliegen der Wirtschaft. Durch eine umfangreiche Berichterstattung in den Medien und durch parlamentarische Anfragen von Abgeordneten ist diese Thematik im Berichtszeitraum öffentlich intensiv diskutiert worden.

Der Landesbeauftragte für den Datenschutz hat schon in den vergangenen Jahren darauf hingewirkt, daß bei derartigen Sicherheitsüberprüfungen die Datenschutzbelange der davon betroffenen Bürger weitestmöglich berücksichtigt werden.

Zur datenschutzrechtlichen Zulässigkeit derartiger Sicherheitsüberprüfungen ist folgendes festzustellen:

Vorweg stelle ich klar, daß der Landesbeauftragte für den Datenschutz entgegen teilweise anderslautender Berichterstattung in den Medien die bisher durchgeführten Sicherheitsüberprüfungen in der Privatwirtschaft nicht als „rechtswidrig" bezeichnet hat. Es entzieht jeder sachlichen Diskussion die Grundlage, wenn Antwortschreiben des Datenschutzbeauftragten sinnentstellt und verfälscht in der Öffentlichkeit wiedergegeben werden. Rechtmäßigkeit oder Rechtswidrigkeit von Datenverarbeitungsmaßnahmen im Zusammenhang mit Sicherheitsüberprüfungen kann der Datenschutzbeauftragte in der Regel nur nach Überprüfung des jeweiligen Einzelfalls, nicht jedoch global feststellen.

Zum Grundsätzlichen ist hier folgendes zu sagen:

Zwar gibt es derzeit noch keine besonderen gesetzlichen Regelungen für Sicherheitsüberprüfungen in der Privatwirtschaft, in denen der Verfahrensablauf, die am Verfahren beteiligten Behörden, die notwendigen Datenübermittlungen und der Umfang der zu speichernden Daten festgelegt werden. Entsprechende Regelungen sind in Vorbereitung. Das macht die Sicherheitsüberprüfung, wie sie derzeit praktiziert wird, aber nicht rechtswidrig. Nach Art. 2 Abs. 2 Ziffer 2 des Gesetzes über die Errichtung eines Landesamtes für Verfassungsschutz ist dem Landesamt die Mitwirkung beim Sabotageschutz in der Privatwirtschaft als Aufgabe zugewiesen. Darüber hinaus bestehen Richtlinien zum Verfahren der Sicherheitsüberprüfung. Bei dieser Gesetzeslage sind bei der Durchführung einer Sicherheitsüberprüfung in der Privatwirtschaft, insbesondere für die hierbei notwendigen Datenerhebungen und -übermittlungen im öffentlichen Bereich, folgende Grundsätze zu beachten:

Aus dem Recht auf informationelle Selbstbestimmung ergibt sich, daß derzeit eine solche Sicherheitsüberprüfung nur mit der ausdrücklichen Einwilligung des Betroffenen erfolgen darf.

Für eine gesetzliche Regelung des Verfahrens der Sicherheitsüberprüfungen werden folgende Grundsätze zu berücksichtigen sein: Das Verfahren muß für den Betroffenen durchschaubar sein. Der Bewerber ist nach Möglichkeit zumindest in groben Zügen über das Ergebnis der ihn betreffenden Sicherheitsüberprüfung zu unterrichten, wenn es für die Entscheidung über die Einstellung auf das Ergebnis der Überprüfung durch die Sicherheitsbehörden ankommt. Keine Unterrichtung ist geboten, wenn der Bewerber beispielsweise aus fachlichen Gründen nicht eingestellt wird. Grundsätzlich, d.h. wenn keine Sicherheitsbedenken entgegenstehen, sollte ihm auch Gelegenheit zur Stellungnahme zu für ihn nachteiligen Erkenntnissen gegeben werden, damit er bei Personenverwechslungen oder offensichtlichen Fehleinschätzungen der Sicherheitsbehörden – ggf. durch Einschaltung des Landesbeauftragten für den Datenschutz – die Informationen berichtigen lassen kann. Von einer derartigen Unterrichtung des Betroffenen durch die Firma sollte nur in eng umschriebenen Fällen abgesehen werden. In diesen Fällen sollte aber der Datenschutzbeauftragte vom Landesamt über die Sicherheitsbedenken unterrichtet werden, damit wenigstens er den Vorgang überprüfen kann.

Das Landesamt für Verfassungsschutz hat sich bereit erklärt, schon heute im wesentlichen bezüglich der Unterrichtung des Datenschutzbeauftragten so zu verfahren. So werden die Unternehmen der Privatwirtschaft aufgefordert, den Betroffenen bei Vorliegen von Sicherheitsbedenken auf die Möglichkeit einer Anrufung des Landesbeauftragten für den Datenschutz hinzuweisen.

Der Grundsatz der Verhältnismäßigkeit gebietet, daß eine Sicherheitsüberprüfung erst dann eingeleitet wird, wenn die Beschäftigung des Bewerbers in einem sicherheitsrelevanten und sabotagegefährdeten Bereich oder eine Befassung mit entsprechenden Vorgängen ernsthaft in Betracht kommt. Das heißt, daß alle anderen Voraussetzungen für eine Einstellung oder Umsetzung im Betrieb bereits abgeklärt sein sollten, bevor die Sicherheitsüberprüfung durchgeführt wird. Der Grundsatz der Verhältnismäßigkeit erfordert außerdem, daß die sicherheitsempfindlichen Bereiche, für die Sicherheitsüberprüfungen vorausgesetzt werden, auf das erforderliche Maß eingegrenzt und möglichst genau beschrieben werden. Damit wird auch die Zahl der zu überprüfenden Personen im Interesse der davon betroffenen Bürger wie auch der damit befaßten Behörden auf das tatsächlich erforderliche Maß verringert. Allerdings kann der Landesbeauftragte für den Datenschutz den Unternehmen die Verantwortung für die Sicherheit ihrer Betriebe nicht abnehmen. Wenn ein Betrieb eine Sicherheitsüberprüfung nach sorgfältiger Prüfung für erforderlich hält, und

keine offensichtliche Fehleinschätzung vorliegt, kann eine solche Praxis nicht beanstandet werden.

Ein Abgeordneter hat über die Medien berichtet, daß ihm 5 Fälle von Sicherheitsüberprüfungen bekannt seien, in denen offenbar Zweifel an der Zulässigkeit der Maßnahmen bestünden. Ich habe mich schriftlich an den Abgeordneten gewandt und meine Bereitschaft erklärt, datenschutzrechtliche Überprüfungen vorzunehmen. Auf meine Bitte, hierzu nähere Hinweise auf die gerügten Fälle zu geben, hat der Abgeordnete noch nicht geantwortet. Unabhängig davon beabsichtige ich jedoch, die seit 1. August 1987 durchgeführten Sicherheitsüberprüfungen für die Privatwirtschaft beim Landesamt für Verfassungsschutz im Verlauf des Jahres 1988 zu überprüfen.

5.3. Bereichsspezifische Datenschutzregelungen bei Nachrichtendiensten

Zur Notwendigkeit der Schaffung bereichsspezifischer Datenschutzregelungen für die personenbezogene Datenverarbeitung durch Nachrichtendienste habe ich mich im letzten Tätigkeitsbericht geäußert. Über diese Notwendigkeit der Schaffung präziser gesetzlicher Regelungen besteht auch allgemeine Übereinstimmung. Bis zur Schaffung dieser Gesetze sind die bereits bisher bestehenden Normen als Maßstab heranzuziehen oder ist auf die Einwilligung des Betroffenen abzustellen, soweit dies im Einzelfall ein praktikabler Weg ist.

Das Fehlen eindeutiger gesetzlicher Grundlagen für die Tätigkeit von BND und MAD zeigt sich in Bayern besonders stark, weil der Gesetzgeber die datenschutzrechtliche Zulässigkeit von Datenübermittlungen an andere öffentliche Stellen (z. B. an BND und MAD) in Art. 17 Abs. 1 BayDSG ausdrücklich an das Vorliegen einer durch Rechtsnorm zugewiesenen Aufgabe knüpft. Soweit z. B. der MAD für die von ihm durchzuführenden Sicherheitsüberprüfungen über Anghörige der Bundeswehr Daten aus dem Schulbereich benötigt, ist deshalb auf die Einwilligung des zu Überprüfenden für die Datenübermittlung von den Schulen an den MAD abzustellen. Entsprechendes ist mit dem MAD vereinbart. In anderen Fällen, in denen sich aus der Natur der Sache das Erholen einer Einwilligung der Betroffenen verbietet, können Datenübermittlungen von bayerischen Behörden an diese Dienste nur unter Abwägung der Sicherheitsbelange einerseits und der schutzwürdigen Belange des Betroffenen andererseits vorgenommen werden, soweit die Datenübermittlungen nicht im Einzelfall nach § 72 SGB X, § 35 Abs. 1 StVG oder Art. 31 MeldeG zulässig sind.

6. Justiz

6.1. Überblick

Im Justizbereich bahnt sich ein Wandel an, der auch für den Datenschutz nicht ohne Auswirkungen bleiben wird. Bis vor wenigen Jahren hat gerichtliche und staatsanwaltschaftliche Tätigkeit nahezu ausschließlich in Akten ihren Niederschlag gefunden. Karteien hatten fast nur Hilfsfunktionen. Jetzt hält der Computer auch im Justizbereich Einzug. Im Berichtszeitraum sind mir eine Reihe neuer **Automatisierungsvorhaben** angekündigt oder gemeldet worden.

- Gemeldet wurden Verfahren zur Büroautomatisation für die Geschäftsstellen in Zivilsachen, zur Unterstützung der Führung des Grundbuches und zur automatisierten Führung von Schuldnerverzeichnis und Vollstreckungsregister.
- In der Strafgerichtsbarkeit wurden Überlegungen zum Aufbau eines länderübergreifenden staatsanwaltschaftlichen Informationssystems bekannt.
- Für die Justizvollzugsanstalten wurden automatisierte Verfahren zur Abwicklung des Lastschrifteinzugsverfahrens für wiederkehrende Einzahlungen und für die Verwaltung von Gefangenengeldern entwickelt. Ein weiteres neues Verfahren ermöglicht die Übermittlung von Gefangenendaten zum DV-System der Alarm- und Kommunikationsanlagen.
- Das Staatsministerium der Justiz kündigte ferner die Errichtung einer DV-Personaldatei an.
- Auch die Aufgaben des Justizprüfungsamtes sollen künftig DV-unterstützt abgewickelt werden.

Datenschutzkontrolle

Die derzeitige Entwicklung der Automatisation in der bayerischen Justiz ist in erster Linie vom Einsatz dezentraler, arbeitsplatzbezogener, mehrplatzfähiger Kleincomputer mit standardisierten Betriebssystemen gekennzeichnet. Die zunehmende Automatisierung auf allen Ebenen macht eine ständige begleitende Datenschutzkontrolle erforderlich. Im Berichtszeitraum konnte ich dabei die betroffenen Justizbehörden immer wieder auf datenschutzrechtliche Probleme und Anforderungen hinweisen. Die Diskussion verlief stets sachlich und konstruktiv.

Wegen der zunehmenden Automatisierung habe ich mich im Berichtszeitraum wiederholt vor Ort über den Einsatz der Datenverarbeitung in der Justiz informiert. So habe ich ein Grundbuchamt und das dort geführte automationsgestützte Grundbuch besichtigt und eine Staatsanwaltschaft datenschutzrechtlich **überprüft.**

Gesetzgebung

Das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 (BVerfGE 65, 1 ff) hat auch in der Justiz zu einer intensiven Diskussion über die Erforderlichkeit neuer **gesetzlicher Vorschriften** über die Erhebung und Verarbeitung personenbezogener Daten geführt. Die Überlegungen zur Reform des Strafprozeßrechts, zur Regelung des Justizmitteilungswesens, zur Novellierung des Strafvollzugsgesetzes sowie zur Änderung der Vorschriften über das Schuldnerverzeichnis in der Zivilprozeßordnung (§ 915 ZPO) sind im Berichtszeitraum weiter fortgeführt worden. Im Rahmen der mir zugewiesenen Kompetenzen habe ich mich zu vielen Vorschlägen geäußert. Ein wesentliches Anliegen war mir dabei klarzustellen, in welchen Fragen eine Neuregelung aus Gründen des Persönlichkeitsschutzes und der verfassungsrechtlichen Vorgaben unbedingt geboten ist. Mein Bestreben war es, den notwendigen Datenschutz zu gewährleisten, einseitige überzogene Regelungen indes zu vermeiden.

Eingaben

Neben den Themenbereichen Automatisation und Gesetzgebung hatte ich mich im Berichtszeitraum wiederum mit zahlreichen **Bürgereingaben** zum Persönlichkeitsschutz in staatsanwaltschaftlichen und gerichtlichen Verfahren zu

befassen. Vereinzelt haben mich auch Eingaben zum Thema Datenschutz im Notariat erreicht. Gegenstand dieser Eingaben war im wesentlichen stets der Vorwurf, der Notar habe seine ihm vom Gesetz auferlegte Verschwiegenheitspflicht verletzt. In allen Fällen konnte – ohne daß ich meine Prüfkompetenz in Anspruch genommen habe – im Benehmen mit den zuständigen Aufsichtsbehörden eine Klärung herbeigeführt werden. In keinem Falle war eine Beanstandung auszusprechen.

Vielfach wandten sich, wie schon in den vergangenen Jahren, Strafgefangene mit ihren Anliegen an meine Dienststelle. Ein weiterer Problembereich war die Weitergabe personenbezogener Daten durch Justizbehörden an Personen oder Einrichtungen, die sich mit der Durchführung kriminologischer Forschungsvorhaben befassen.

6.2. Automatisierungsvorhaben

6.2.1. Errichtung eines länderübergreifenden staatsanwaltschaftlichen Informationssystems

Ein aus meiner Sicht besonders bedeutsames Automatisierungsvorhaben der Justiz ist die Errichtung eines länderübergreifenden staatsanwaltschaftlichen Informationssystems. Die Planungen der Justiz befinden sich allerdings noch im Anfangsstadium; derzeit liegt noch kein geschlossenes Konzept vor. Grundgedanke des Informationssystems ist, daß die Staatsanwaltschaften Daten Beschuldigter aus einem Strafverfahren personenbezogen in automatisierter Form zum Zugriff für weitere, an das System angeschlossene Strafverfolgungsbehörden bereitstellen, die die Daten dann in anderen Verfahren nutzen können. Der Datensatz sowie die näheren Einzelheiten des Verfahrens, insbesondere auch zur Datensicherung, stehen noch nicht fest.

Obwohl sich damit ein mögliches DV-Verfahren, an das die Meßlatte des Datenschutzes anzulegen ist, bisher erst in Umrissen abzeichnet, halte ich es für sinnvoll, bereits im Planungsstadium im Benehmen mit anderen Datenschutzbeauftragten grundlegende Überlegungen zum Datenschutz zu entwickeln und an das Staatsministerium der Justiz heranzutragen.

Nach meiner Auffassung stehen verfassungsrechtliche Grundsätze des Datenschutzes der Errichtung eines länderübergreifenden staatsanwaltschaftlichen Informationssystems nicht entgegen. Die schutzwürdigen Belange der Betroffenen können durch eine entsprechende Ausgestaltung des Informationssystems und geeignete technisch-organisatorische Maßnahmen gewahrt werden.

Gegen ein eigenes staatsanwaltschaftliches Informationssystem spricht auch nicht, daß die Polizei bereits heute automatisierte Informationssysteme unterhält, die in der Praxis ebenfalls der Strafverfolgung dienen. Zum einen sind in diesen Systemen nicht alle Strafverfahren erfaßt, da die Staatsanwaltschaft nicht ausnahmslos die Polizei mit der Durchführung der erforderlichen Ermittlungen beauftragt, wenn sie vom Verdacht einer Straftat Kenntnis erlangt hat. Vor allem aber überträgt die Strafprozeßordnung die Leitung des Ermittlungsverfahrens eindeutig der Staatsanwaltschaft. Als „Herr des Verfahrens" darf die Staatsanwaltschaft nicht von der Nutzung technischer Instrumente ausgeschlossen und auf den Informationsstrang der Polizei verwiesen werden. Sie muß in der Lage sein, in Wahrnehmung der ihr gesetzlich zugewiesenen Aufgaben auch von den Möglichkeiten der modernen Datenverarbeitung Gebrauch zu machen.

Wichtig ist allerdings, daß die verschiedenen Informationssysteme bei Polizei und Staatsanwaltschaft künftig nicht unabhängig voneinander weiterentwickelt und betrieben werden. Ziel der Überlegungen muß ein zukunftsweisendes, abgestimmtes Gesamtkonzept der Informationsverarbeitung im Strafverfolgungsbereich sein.

6.2.2. Automationsunterstützung der Personalverwaltung

Das Staatsministerium der Justiz plant die Einführung eines DV-Verfahrens zur Unterstützung der Personalverwaltung. Der Datensatz stellt einen Auszug aus den Personalakten der Bediensteten dar. Das Verfahren soll die Personalakten nicht etwa ersetzen, sondern lediglich eine schnelle Auswertung und einen raschen Zugriff ermöglichen und bisher geführte Listen u. ä. überflüssig machen.

Meine Dienststelle wurde vom Staatsministerium der Justiz bereits in einem sehr frühen Planungsstadium eingeschaltet, so daß meine Stellungnahme zu einigen datenschutzrechtlichen Fragen in der weiteren Diskussion, die sehr offen und konstruktiv geführt wurde, problemlos mit berücksichtigt werden konnte. Beispielsweise habe ich mich zur inhaltlichen Ausgestaltung bestimmter Datenfelder (Religion, Familienstand etc.) kritisch geäußert. Bedenken hatte ich vor allem gegen die m. E. zu umfassende Speicherung von Beurteilungen vorgetragen. Die offenen Fragen konnten jedoch im gegenseitigen Einvernehmen geklärt werden. So erwägt das Staatsministerium der Justiz jetzt, auf eine weitere Speicherung von Probezeitbeurteilungen nach Erfassung der ersten periodischen Beurteilung des Betroffenen zu verzichten. Ich habe meinerseits meine Bedenken gegen eine historische Erfassung weiterer Beurteilungen zurückgestellt, wobei ich davon ausgehe, daß in der Regel nicht mehr als vier periodische Beurteilungen im System erfaßt werden.

Nach dem derzeitigen Stand der Erörterungen sind datenschutzrechtliche Einwände gegen das geplante System nicht mehr zu erheben. Zu klären bleibt noch die Frage der Datensicherung. Hierzu will sich das Staatsministerium der Justiz noch gesondert äußern.

6.2.3. Sonstige Automatisationsvorhaben

Über eine Vielzahl weiterer Automatisationsvorhaben der Justiz habe ich im Überblick kurz berichtet. Ein besonders wichtiges Kriterium für die Beurteilung eines Verfahrens ist für mich dabei stets die Sensibilität der zu verarbeitenden Daten. Sensible Daten sind vor allem Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen (vgl. § 27 Abs. 3 Satz 3 BDSG). Die Sensibilität der Daten ist vor allem dann von Bedeutung, wenn die Daten im Auftrag der speichernden Stelle durch andere Stellen, etwa durch Privatfirmen, verarbeitet werden sollen. Eine Auftragsdatenverarbeitung durch Private halte ich datenschutzrechtlich in der Regel nur dann für unbedenklich, wenn die betroffenen Daten nicht sensibler Natur sind.

6.3. Datenschutzrechtliche Prüfung einer Staatsanwaltschaft

Mein besonderes Interesse galt dem seit 1.1.1985 automatisiert geführten Zentralen Namensverzeichnis (ZNV) der Behörde. Dieses Namensverzeichnis ist ein Hilfsmittel zur Führung der Akten, mit dessen Hilfe der Name eines Beschuldigten (bzw. eines Geschädigten, wenn der Name des Täters unbekannt ist) einem bestimmten Verfahren zugeordnet werden kann. Die Datei enthält darüber hinaus noch weitere Datenfelder zur näheren Identifizierung des Betroffenen, zum Tatvorwurf und zur Erledigung des Verfahrens.

Die Prüfung hat im Ergebnis gezeigt, daß die geprüfte Staatsanwaltschaft dem Vollzug datenschutzrechtlicher Bestimmungen großes Gewicht beimißt. Wesentliche Verstöße gegen das Datenschutzrecht waren erfreulicherweise nicht zu verzeichnen. Dennoch hat die Prüfung aus datenschutzrechtlicher Sicht Anlaß zu Bemerkungen gegeben:

Im wesentlichen berücksichtigt hat die Staatsanwaltschaft meine Anregung, bei einer erheblichen Abweichung des im ZNV eingetragenen Tatvorwurfs vom tatsächlichen Ergebnis der Ermittlungen eine inhaltliche Berichtigung des Registereintrags vorzunehmen. Die Sachbearbeiter wurden angewiesen, dementsprechend zu verfahren.

Etwa 20 bis 30 % der Ermittlungsverfahren werden von der Staatsanwaltschaft nach § 170 Abs. 2 StPO eingestellt, weil die Ermittlungen keinen genügenden Anlaß zur Erhebung der öffentlichen Klage bieten. Durch eine solche Einstellung werden die Beschuldigten vom zunächst bestehenden Schuldvorwurf entlastet. Obwohl die Staatsanwaltschaft im ZNV zahlreiche Erledigungsarten speichert, wird aus arbeitsökonomischen Gründen auf die Speicherung dieser häufigen, den Betroffenen zudem entlastenden Erledigungsart seit einiger Zeit weitgehend verzichtet. Der Datensatz des Beschuldigten kann ohne Hinweis auf diese Verfahrenseinstellung zu Fehlbeurteilungen führen, weil unklar bleibt, ob und ggf. wie das Verfahren bereits abgeschlossen werden konnte. Ich habe deshalb datenschutzrechtliche Bedenken wegen der fehlenden Speicherung dieser Erledigungsart geäußert. Bei den Planungen für ein Gesamtkonzept zur Unterstützung des Geschäftsbetriebes in Strafsachen wird nun die Einführung eines eigenen Kennzeichens für diese Form der Verfahrenserledigung angestrebt. Dies begrüße ich nachdrücklich.

Nicht ausgeräumt werden konnten meine Bedenken, die sich auf folgende Feststellungen stützen: Bis Ende 1985 wurden im ZNV der geprüften Staatsanwaltschaft Verfahrenserledigungen durch Einstellungen nach § 170 Abs. 2 StPO durch ein gesondertes Erledigungskennzeichen („C") erfaßt. Dieses Kennzeichen hat nach dem Fortfall der generellen Kennzeichnung aller Einstellungen nach § 170 Abs. 2 StPO (siehe oben) eine andere Bedeutung erlangt und weist nun auf eine Einstellung wegen Schuldunfähigkeit hin. Dennoch wurden Eintragungen, bei denen früher das (jetzt nicht mehr zutreffende) Kennzeichen „C" vergeben wurde, nicht berichtigt, so daß das Register in diesen Fällen nunmehr einen sachlich unzutreffenden Eindruck über den Grund für die Verfahrenseinstellung vermittelt.

Meiner Anregung, eine Überprüfung und nachträgliche Berichtigung vorzunehmen, wurde nicht entsprochen, da der damit verbundene Arbeitsanfall erheblich sei und die Kennzeichnung sich auf den gespeicherten Bürger nicht belastend auswirke, da ohne Beiziehung der Akten eine Sachbehandlung nicht erfolge.

Ich bedauere diese Entscheidung, zumal der Aufwand für eine Überprüfung wegen des verhältnismäßig kurzen Zeitraums, in dem das Kennzeichen „C" in seiner ursprünglichen Bedeutung vergeben wurde, m. E. nicht so sehr ins Gewicht fallen dürfte. Hilfsweise wäre aber noch in Betracht zu ziehen, alle Sachbearbeiter der Staatsanwaltschaft ins Auge fallend deutlich darauf hinzuweisen, daß bei der Verwertung von Auszügen aus dem ZNV mit Erledigungskennzeichen „C" wegen des Bedeutungswandels dieses Schlüssels besondere Sorgfalt zu beachten ist.

6.4. Gesetzgebung

6.4.1. Strafprozeßordnung

Die Datenschutzbeauftragten des Bundes und der Länder haben gemeinsam aus datenschutzrechtlicher Sicht klarzustellen versucht, wo bisher hinreichende Rechtsgrundlagen für die Datenverarbeitung im Strafverfahren fehlen und welchen inhaltlichen Anforderungen zum Schutze des informationellen Selbstbestimmungsrechts Betroffener die neuen Vorschriften genügen sollten. Diese gemeinsame Stellungnahme der Datenschutzbeauftragten befaßt sich insbesondere auch mit den Befugnisnormen der Strafverfolgungsbehörden zur Informationserhebung im Ermittlungsverfahren und berührt dabei Fragen der Fahndung wie z. B. die Zulässigkeit von Rasterfahndung oder polizeilicher Beobachtung, den Einsatz von Spurendokumentationssystemen oder den Einsatz technischer Geräte zur Informationsgewinnung. Weitere Bereiche, die angesprochen werden, sind vor allem die Speicherung und weitere Nutzung der gewonnenen Daten (einschließlich der Errichtung von Informationssystemen).

Viele Anregungen der Datenschutzbeauftragten, die hier im einzelnen nicht wiedergegeben werden können, wurden im vom Bundesminister der Justiz vorgelegten „Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren" (Stand 31.7.1986) bereits aufgegriffen. Der Entwurf will auch weiterhin grundsätzlich an dem für die Strafprozeßordnung bisher kennzeichnenden System der Einzelermächtigung festhalten.

Zudem hat der Arbeitsentwurf mittlerweile durch einen weiteren Entwurf des Bundesministers der Justiz für „Allgemeine Bestimmungen über die Speicherung, Verwendung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden" (Stand: 16.7.1987) eine Ergänzung erfahren. Dieser Entwurf enthält Rechtsgrundlagen für die Speicherung und weitere Nutzung von Daten zu Strafverfolgungszwecken in verfahrensbezogenen und verfahrensübergreifenden Dateien. Weitere Bestimmungen betreffen die Errichtung von Dateien für die Vorgangsverwaltung und die Mitteilungen über den Verfahrensausgang an die Polizei.

Eine Stellungnahme zu diesem Entwurf werde ich in den nächsten Wochen wiederum in Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der anderen Länder erarbeiten. Schon jetzt kann ich – ohne auf Details näher einzugehen – grundsätzlich begrüßen, daß der

Entwurf zumindest dem wesentlichen Anliegen der Datenschutzbeauftragten entgegenkommt, über ein nur punktuelles Herausgreifen einiger weniger Bereiche hinaus eine weitergehende Regelung der Informationsverarbeitung im Strafprozeß herbeizuführen.

Ein wesentliches Problem sehe ich allerdings auch weiterhin in der Abstimmung der neuen StPO-Bestimmungen mit dem Polizeirecht, ohne die ein effizienter Gesetzesvollzug durch die Strafverfolgungsbehörden kaum denkbar ist. Besonderes Augenmerk wird auch darauf zu legen sein, daß das gesetzliche Regelwerk nicht durch eine Flut von perfektionistischen Detailregelungen unvollziehbar wird. Das ZEVIS-Gesetz sollte hier warnendes Beispiel sein.

6.4.2. Justizmitteilungsgesetz

Mit den Mitteilungen in Straf- und Zivilsachen werden viele sensible Daten aus dem Bereich der Justiz an andere Stellen übermittelt. Der Bundesminister der Justiz hat einen ersten Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz) vorgelegt. Der Entwurf, der sich noch als Diskussionsgrundlage versteht, sieht Rechtsgrundlagen für personenbezogene Mitteilungen der Justizbehörden über Zivil- und Strafverfahren an dritte Stellen vor, die derzeit im wesentlichen aufgrund der Anordnung über Mitteilungen in Strafsachen (MiStra) und der Anordnung über Mitteilungen in Zivilsachen (MiZi) vorgenommen werden.

Aus datenschutzrechtlicher Sicht habe ich die Vorlage des Entwurfs eines Justizmitteilungsgesetzes grundsätzlich begrüßt. Der Entwurf muß als erster konkreter Schritt auf dem Weg zu einer verfassungsrechtlich unumgänglich gewordenen gesetzlichen Verankerung des Mitteilungswesens im Justizbereich gesehen werden. Ferner entsprechen die vom Entwurf vorgesehene Pflicht zur Benachrichtigung des Betroffenen sowie die Betonung des Zweckbindungsgrundsatzes den immer wieder erhobenen Forderungen der Datenschutzbeauftragten. Die weitere Entwicklung dieses Gesetzgebungsvorhabens werde ich mit besonderem Interesse verfolgen.

6.4.3. Strafvollzugsgesetz

Auch über die Überlegungen zu einer datenschutzrechtlichen Ergänzung des Strafvollzugsgesetzes habe ich in meinem 8. Tätigkeitsbericht berichtet. Zwischenzeitlich hat der Bundesminister der Justiz einen ersten Arbeitsentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes (Stand: 31.3.1987) vorgelegt. Er enthält allgemeine Regelungen über die Erhebung und Nutzung personenbezogener Daten im Vollzugsbereich.

Aus datenschutzrechtlicher Sicht muß vor allem kritisiert werden, daß die Vorschriften des Entwurfs über die verschiedenen Formen der Datenverarbeitung in der Justizvollzugsanstalt zu unsystematisch geraten sind. Die Zusammenhänge bleiben oft unklar. Der Phase der Datenspeicherung wurde zu wenig Beachtung geschenkt.

Auf eine nähere Bewertung des Entwurfs habe ich bisher verzichtet, nachdem mir bekannt wurde, daß der Entwurf von den Landesjustizverwaltungen bereits jetzt überwiegend abgelehnt wird. Die Praxis sieht die vorgeschlagenen Regelungen als nicht praktikabel an. Der Bundesminister der Justiz hat den Auftrag, auf der Grundlage der bisherigen Beratungen einen neuen Entwurf vorzulegen. Dies bleibt vorläufig abzuwarten.

6.4.4. Schuldnerverzeichnis

Die Bemühungen zur Änderung der gesetzlichen Vorschriften über das Schuldnerverzeichnis (§ 915 ZPO) wurden im Berichtszeitraum wieder aufgenommen. Der Bundesminister der Justiz hat einen neuen Gesetzentwurf (Stand: 28.8.1987) vorgelegt, der in vielen Punkten eine Verbesserung der bisher diskutierten Vorschläge darstellt.

Gegenstand des Entwurfs ist die Regelung der Speicherung und weiteren Nutzung von Daten im Schuldnerverzeichnis der Amtsgerichte. Dort werden die Personen eingetragen, die die eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die wegen Nichtabgabe der eidesstattlichen Versicherung Haft angeordnet ist.

Als problematisch haben sich in der Vergangenheit vor allem die regelmäßige Abgabe von Informationen aus dem Schuldnerverzeichnis an Dritte und die weitere Verarbeitung der Daten bei diesen Stellen erwiesen. Der Entwurf sieht zur Wahrung der schutzwürdigen Belange der Betroffenen einige Schranken und Schutzvorkehrungen vor. Neu ist zum Beispiel der Vorschlag, alle Empfängerstellen, die nicht bereits der strengen Datenschutzkontrolle für den öffentlichen Bereich unterstehen, nicht nur der Anlaßkontrolle, sondern der generellen Überwachung durch die zuständigen Aufsichtsbehörden zu unterwerfen.

Ich habe mich in meiner Stellungnahme gegenüber dem Staatsministerium der Justiz zum Entwurf grundsätzlich positiv geäußert. Trotz mancher Verbesserungen habe ich allerdings nach wie vor Bedenken, ob die Einhaltung der Datenschutzvorschriften, vor allem über die Löschung überholter Eintragungen, bei den Beziehern von Listen aus dem Schuldnerverzeichnis in der Praxis hinreichend gewährleistet werden kann. Ich befürchte, daß ohne besondere Sicherungsmaßnahmen veraltete Listen mit längst überholten belastenden Eintragungen unter den Kreditgebern kursieren werden. Dennoch hoffe ich, daß dieses Gesetzesvorhaben, bei dem die Interessen des Gläubigerschutzes wie des Datenschutzes sorgsam gegeneinander abgewogen werden müssen, baldmöglichst zum Abschluß gebracht werden kann.

7. Städte, Gemeinden, Landratsämter

7.1. Neuer Personalausweis, Doppelvergabe von Seriennummern

Seit 1. April 1987 werden die neuen Personalausweise ausgegeben. Jeder Ausweis trägt eine nur einmal zu vergebende Seriennummer. Sie besteht aus einer vierstelligen Behördenkennzahl, einer fünfstelligen laufenden Nummer und einer Prüfziffer.

Ende November 1987 wurde bekannt, daß in einer Reihe von Fällen Seriennummern doppelt vergeben worden sind. Meine ersten Prüfungen haben ergeben, daß die Ursachen für diese Doppelvergaben zum Teil bei den Personalausweisbehörden, zum Teil bei der Bundesdruckerei liegen.

In zahlreichen von der Bundesdruckerei gemeldeten Fällen waren jedoch Seriennummern nicht wirklich doppelt vergeben worden. Um keine Doppelvergabe handelt es sich

nämlich, wenn ein Ausweis für die gleiche Person, z. B. wegen eines Schreibfehlers, zweimal hergestellt werden mußte.

Im übrigen zeigten sich bei einigen Stichproben folgende Fehlerquellen:

- Die Bundesdruckerei lieferte an Gemeinden zunächst eine Liste mit 30 Personalausweis-Seriennummern für Testzwecke. Die Verwendung dieser Nummern wurde für den Echtbetrieb, also für die tatsächliche Ausstellung neuer Personalausweise, ausdrücklich zugelassen. Nachdem die ersten 30 Seriennummern vergeben waren, bestellten die von mir geprüften Gemeinden eine neue Liste. Die Bundesdruckerei schickte daraufhin – zumindest in mir bekannt gewordenen Fällen – Listen, die nochmals die ersten 30 bereits zu Probezwecken (und zur Echtvergabe) übermittelten Seriennummern enthielten.

  Einige Personalausweisbehörden erkannten offenbar nicht, daß die Nummern nochmals geliefert worden waren und vergaben sie ein zweites Mal. Die Doppellieferung fiel wohl deshalb nicht auf, weil die Seriennummern auf den ersten Blick nicht als eine aufsteigend sortierte Reihenfolge von Zahlen erkennbar waren. Bei genauerer Prüfung anhand des der Gemeinde bekannten Aufbaus der Seriennummer wäre die Doppelvergabe zweifellos vermeidbar gewesen.

- In anderen von mir überprüften Fällen hat die Personalausweisbehörde die vergebene Seriennummer versehentlich nicht in der Seriennummernliste gekennzeichnet. Nach Rücklauf der Personalausweise von der Bundesdruckerei ist ein Abgleich der Personalausweise mit der Seriennummernliste in einigen Gemeinden unterblieben. Die Seriennummer, deren Vergabe nicht registriert worden war, wurde später nochmals vergeben.

  Die Personalausweisbehörden sind vielfach als selbstverständlich davon ausgegangen, daß die Bundesdruckerei schon bei Eingang der Anträge die darin eingetragenen Seriennummern mit den bei der Bundesdruckerei als vergeben registrierten Seriennummern vergleicht und den Antrag im Falle einer Doppelvergabe zurücksendet.

Die Unannehmlichkeiten für die Bürger hätten sich freilich weitgehend vermeiden lassen, wenn die Bundesdruckerei die Prüfung auf Doppelvergabe der Seriennummern nicht erst bei der späteren Abrechnung mit den Gemeinden, sondern bereits bei Eingang des Antrags vorgenommen hätte. Gründe des Datenschutzes hätten dem nicht entgegengestanden.

Das Staatsministerium des Innern hat mir mitgeteilt, es habe den Personalausweisbehörden inzwischen Hinweise zur Bereinigung bisheriger und zur Vermeidung künftiger Doppelvergaben gegeben.

Die Doppelvergabe von Seriennummern ist für die betroffenen Bürger zweifellos lästig, weil ein neuer Ausweis ausgestellt werden muß. Datenschutzrechtliche Nachteile sind ihnen aber nach derzeitiger Erkenntnis nicht entstanden.

7.2. Unzulässige Verwendung von Steuerdaten für andere Zwecke der Gemeinde

Unter dieser Überschrift wurde bereits im 7. und 8. Tätigkeitsbericht darauf hingewiesen, daß Gemeinden personenbezogene Daten wie Namen, Anschrift und Objekt (Grundstück) eines Steuerpflichtigen aus gemeindlichen Steuerunterlagen auch für andere gemeindliche Zwecke verwenden. Im Berichtszeitraum wurden mir weitere Fälle einer Nutzung von Besteuerungsunterlagen bekannt:

- Die Brandversicherungsämter der Bayerischen Versicherungskammer erhielten in der Vergangenheit von den gemeindlichen Steuerämtern die Anschriften von Grundstückseigentümern.

- Eine bayerische Stadt wollte in einem neu zu entwickelnden DV-Verfahren die Übermittlung von Namen und Anschriften aus Steuerunterlagen an das städtische Bauverwaltungsamt vorsehen.

  In beiden Fällen hat der Landesbeauftragte darauf hingewiesen, daß das Steuergeheimnis (§ 30 der Abgabenordnung) einer solchen Datenübermittlung entgegensteht.

Eine Verwaltungsgemeinschaft hatte die Frage aufgeworfen, ob das kommunale Steueramt Erkenntnisse, die dort über Gewerbetreibende, vor allem zur Rechtsform der Firma vorliegen, an das kommunale Gewerbeamt weitergeben darf. Hierzu hat das Staatsministerium des Innern folgendermaßen Stellung genommen:

„Adreß- und Objektdaten, die in einem Verfahren in Gewerbesteuersachen bekanntgeworden sind, unterliegen über § 3 Abs. 2 in Verbindung mit § 1 Abs. 2 Nr. 1 AO dem Steuergeheimnis gem. § 30 AO. Eine Übermittlung dieser Daten an das gemeindliche Gewerbeamt ist wegen der Verletzung des Steuergeheimnisses unzulässig. Unerheblich ist es dabei, ob sich das Gewerbeamt aus steuerlichen oder sonstigen Gründen für die unter das Steuergeheimnis fallenden Daten interessiert. Der Steuerpflichtige ist im Rahmen des Besteuerungsverfahrens verpflichtet, seine für die Besteuerung relevanten Verhältnisse uneingeschränkt zu offenbaren. Daher hat er aber auch einen Anspruch darauf, daß seine Verhältnisse solchen Stellen, die an der Durchführung der Besteuerung nicht beteiligt sind, auch nicht zur Kenntnis gelangen. Die gemeindlichen Gewerbeämter müssen sich daher die für ihre Arbeit benötigten Daten anderweitig beschaffen."

Das Staatsministerium der Finanzen hatte sich bereits früher in gleicher Weise geäußert. Die Verwaltungsgemeinschaft wurde auf diese Rechtslage hingewiesen.

Bezüglich der Verwendung von Grundsteuerdaten für andere Grundstücksabgaben haben sich die obersten Finanzbehörden des Bundes und der Länder allerdings dahin verständigt, schon nach heutiger Rechtslage ergebe die in § 1 Abs. 2 Nr. 1 AO angeordnete entsprechende Anwendung der Abgabenordnung für die Realsteuern, daß die Gemeinden die Steuerdaten auch für andere Grundstücksabgaben verwenden dürften. Das Steuergeheimnis schütze Daten, die in einem Verwaltungsverfahren in Abgabensachen (kommunale Steuern, Gebühren und Beiträge) bekannt geworden sind. Danach könnten die für die Verwaltung der Gebühren und Beiträge erforderlichen

Informationen schon derzeit aus den Grundsteuerdaten entnommen werden.

Das Staatsministerium des Innern hat erneut mitgeteilt, daß erfolgversprechende Verhandlungen zur Änderung der Abgabenordnung in Gang gekommen sind. Der Vorsitzende des Unterausschusses „Kommunale Finanzen" des Arbeitskreises der Länderinnenminister habe den Bundesminister der Finanzen um eine Änderung der Abgabenordnung gebeten. Die Staatsregierung unterstütze nachdrücklich dieses Bemühen um eine Gesetzesänderung.

Die zuständigen obersten Finanzbehörden des Bundes und der Länder bestätigten im September 1987, daß die bestehenden Regelungen der §§ 30, 31 AO einen Steuer-Datenabgleich für Bauordnungs-, Planungs- und Umlageverfahren nicht zuließen. Sie erkannten aber ebenfalls ein Bedürfnis der Gemeinden an, in bestimmten Fällen Daten aus der kommunalen Steuererhebung außerhalb der Abgabezwecke zu verwenden.

Es ist zweifellos sinnvoll und vermeidet unnötige Verwaltungsarbeit und Belästigungen der Bürger, wenn bestimmte, in der Regel wenig sensible Angaben aus den Besteuerungsunterlagen an andere Stellen, die diese Angaben dringend benötigen, weitergegeben werden. Dazu müssen freilich die gesetzlichen Vorschriften geändert werden. Andernfalls müßte die bisherige Datennutzung, auch soweit sie sich auf einige wenige Grunddaten beschränkt, beanstandet und die Änderung einer Vielzahl von DV-Programmen im Bereich des gemeindlichen Steuer- und Abgabenwesens gefordert werden.

7.3. Bekanntgabe des Bauherrn und Entwurfsverfassers

Nach Art. 84 der Bayerischen Bauordnung dürfen die Bauaufsichtsbehörden und die Gemeinden Ort und Straße der Baustelle, Art und Größe des Bauvorhabens sowie Namen und Anschrift des Bauherrn und des Entwurfsverfassers nur veröffentlichen oder an Dritte zum Zweck der Veröffentlichung übermitteln, wenn der Betroffene der Veröffentlichung nicht widersprochen hat.

Bei den Prüfungen in den Bauämtern habe ich festgestellt, daß auf dem Bauantragsformular an der Stelle, wo der Bauwerber und der Entwurfsverfasser ihr Einverständnis zur Veröffentlichung von Daten über den Bau, den Bauherrn und den Entwurfsverfasser erklären können, häufig jegliche Eintragung fehlt. In den Bauämtern wurde mir zwar versichert, daß in diesen Fällen eine Veröffentlichung unterbleibe. Ich habe gleichwohl darum gebeten, bereits bei der Einreichung des Bauantrags zu prüfen, ob Bauherr und Entwurfsverfasser eine Erklärung abgegeben haben. Nur so kann sichergestellt werden, daß Daten aus einem Bauantrag, der hierzu keine Angaben enthält, nicht doch (versehentlich) veröffentlicht werden.

7.4. Bekanntgabe von hypothekarischen Belastungen im Wertgutachten eines Gutachterausschusses

Zwei Grundstückseigentümer haben sich beim Landesbeauftragten darüber beklagt, daß die Geschäftsstelle des Gutachterausschusses einer Stadt im Gutachten über den Verkehrswert von Grundstücken zahlreiche Grundpfandrechte (Hypotheken u.ä.) aufgeführt hat. Auf diese Weise wurde eine Vielzahl am Verfahren beteiligter Personen über die finanziellen Belastungen der Grundstücke der anderen Beteiligten in Kenntnis gesetzt.

Mit dem Staatsministerium des Innern hat der Landesbeauftragte die Ansicht vertreten, daß Grundpfandrechte, die in der Abteilung III des Grundbuches eingetragen werden, in der Regel weder zu den wertbildenden Faktoren, die den maßgeblichen Zustand des Grundstücks bestimmen, noch sonst zu den bei der Wertermittlung zu berücksichtigenden Umständen gehören. Es handelt sich bei diesen Belastungen vielmehr um allgemeine Rechte und Belastungen, die mit der Nutzung des Grundstücks nicht im Zusammenhang stehen und daher regelmäßig keinen Einfluß auf den Verkehrswert haben. Von der Wiedergabe der Grundpfandrechte im Wertgutachten war deshalb abzusehen. Die Bekanntgabe der Belastungsverhältnisse der einzelnen Eigentümer war zur gesetzlich zugewiesenen Aufgabenerfüllung des Gutachterausschusses nicht erforderlich und andererseits geeignet, schutzwürdige Belange der Betroffenen zu beeinträchtigen.

7.5. Verwendung gemeindlicher Unterlagen aus dem Melde- und Standesamt zur Anfertigung einer Ortsstudie

Seit Jahren werde ich immer wieder mit der Frage befaßt, ob interessierte Bürger zur Anfertigung einer geschichtlichen Studie über ihren Wohnort Daten aus Unterlagen des Melde- oder Standesamts erhalten können. Dabei geht es vor allem um Unterlagen, die noch nicht archiviert sind.

Eine umfassende gesetzliche Regelung über die private Nutzung dieser Unterlagen für wissenschaftliche Zwecke besteht bisher nicht. Für Unterlagen des Meldeamtes gilt Art. 34 Meldegesetz. Darin sind sowohl die Voraussetzungen genannt, unter denen eine Auskunft erteilt werden darf, als auch die Daten, die aus dem Melderegister bekanntgegeben werden dürfen. Auskünfte über eine unbestimmte Vielzahl nicht namentlich benannter Einwohner (Gruppenauskunft) sind nur dann zugelassen, wenn für die Zusammensetzung der Personengruppe bestimmte, im einzelnen in Art. 34 Meldegesetz genannte Daten herangezogen werden. Die Volks- oder Religionszugehörigkeit, nach denen beispielsweise bei Studien über „das Dritte Reich" häufig gefragt wird, gehören nicht zu diesen Merkmalen. Eine unmittelbare Einsichtnahme eines Interessenten in das Melderegister ist ausgeschlossen.

Auskünfte über verstorbene und weggezogene Bürger darf das Meldeamt einer Privatperson nur geben, wenn dies zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot unerläßlich ist oder der Betroffene – zu Lebzeiten – schriftlich eingewilligt hat.

Zum Problem der Altdaten aus früheren Melderegistern, die nach dem geltenden Melderecht nicht mehr Inhalt des Melderegisters sein können, verweise ich auf die Ausführungen unter „Einwohnermeldewesen".

Die Personenstandsbücher des Standesamts können für die Erstellung von Ortschroniken, lokalen Studien oder ähnlichem in der Regel nicht verwendet werden. Die Einsichtnahme in diese Bücher ist nach dem Personenstandsgesetz stark eingeschränkt. Das Gesetz sieht nur ein Einsichtsrecht für Vorfahren, Abkömmlinge und Ehegatten vor. Alle anderen Personen müssen zu jedem Personenstandseintrag, den sie einsehen wollen, ein rechtliches

Interesse glaubhaft machen. Ob diese Voraussetzungen vorliegen, hat der Standesbeamte zu prüfen. Die Absicht, eine Chronik zu schreiben, begründet kein rechtliches Interesse. Gleiches gilt für die Erteilung von Auskünften aus den Personenstandsbüchern.

Soweit sich die in Frage stehenden Unterlagen bereits in einem kommunalen Archiv befinden, ist bei der Entscheidung über die Zulässigkeit der Nutzung eine etwa erlassene Benutzungsordnung oder Benutzungssatzung zu berücksichtigen. Die Datenschutzbeauftragten des Bundes und der Länder weisen im übrigen schon seit langem darauf hin, daß die Nutzung archivierter personenbezogener Daten dringend einer gesetzlichen Regelung bedarf. Mittlerweile liegt der Entwurf eines Bayerischen Archivgesetzes vor, der die erforderlichen gesetzlichen Rahmenregelungen auch für den kommunalen Bereich enthält. Näheres zu diesem Gesetzgebungsvorhaben wird im Abschnitt „Archivwesen" berichtet.

7.6. Bearbeitung der Beihilfeangelegenheiten durch den Personalsachbearbeiter

Die staatlichen Beihilfestellen im Geschäftsbereich des Staatsministeriums des Innern sind angehalten, zum Schutz des Persönlichkeitsrechts der Bediensteten auf Referatsebene eine strikte organisatorische und personelle Trennung von Beihilfe und Personalsachbearbeitung durchzuführen. Den Kommunen hat die Staatsregierung empfohlen, entsprechend zu verfahren. Die strikte Trennung von Beihilfe- und Personalsachbearbeitung ist aus der Sicht des Datenschutzes unverzichtbar. Soweit dies aus personellen Gründen nicht möglich ist, muß überlegt werden, ob die Beihilfe nicht über eine Beihilfeversicherung abgewickelt werden kann.

Bei den im Berichtszeitraum vorgenommenen Prüfungen in den Gemeinden zeigte sich, daß dieser Empfehlung der Staatsregierung zur Beihilfeorganisation noch nicht in vollem Umfang entsprochen ist. So wurde in einem Fall festgestellt, daß nach wie vor ein Mitarbeiter im Personalamt die Beihilfeangelegenheiten miterledigt, obwohl er gleichzeitig mit der Personalsachbearbeitung betraut ist. In einem anderen Fall war die Sachbearbeitung in der Beihilfestelle zwar grundsätzlich von der Personalsachbearbeitung getrennt, jedoch wurde für den Beihilfesachbearbeiter im Vertretungsfall eine Dienstkraft der Personalstelle eingesetzt. Es sollte auch ausgeschlossen sein, daß schwierige Beihilfefälle vom Leiter des Personalamtes selbst bearbeitet werden.

8. Einwohnermelderegister

Die ausführliche Diskussion von Fragen des Datenschutzes im Zusammenhang mit der Verarbeitung personenbezogener Daten im Einwohnermelderegister, die sich in früheren Tätigkeitsberichten widerspiegelte, ist inzwischen abgeklungen. Das Meldegesetz vom 24.3.1983, die Meldedaten-Übermittlungs-Verordnung vom 4.12.1984 und die Bekanntmachung des Staatsministeriums des Innern zum Vollzug des Meldegesetzes vom 28.4.1984 sorgten weitgehend für Klarheit. Auslegungsfragen konnten meist in einer sowohl für den Datenschutz wie auch für die Praxis der Verwaltung befriedigenden Weise geklärt werden. Bei der Umsetzung des neuen Melderechts in die tägliche Praxis waren freilich – wie bei umfangreichen neuen Vorschriften nicht anders zu erwarten – teilweise Mängel festzustellen.

Noch nicht befriedigend gelöst ist die Frage, wie mit alten Melderegisterdaten umzugehen ist, die inhaltlich über den in Art. 3 des Meldegesetzes festgelegten Datenrahmen hinausgehen. Zwar werden solche Daten (z.B. Wehrmachts- und RAD-Zeiten, Beruf, Arbeitgeber, Familienverbund bei Volljährigen) korrekterweise nicht mehr in der aktuellen Melde-Kartei bzw. -Datei geführt. Die Frage, ob über diesen Rahmen hinausgehende Altdaten vernichtet werden oder für Nachweiszwecke (z.B. für Rentenzeiten) im Interesse Betroffener oder von Behörden oder lediglich für Forschungszwecke weiter verfügbar sein können, erscheint noch ungeklärt.

8.1. Auskünfte aus dem Melderegister zur Feststellung von Schuldneradressen – Personenverwechslungen

Unter Nr. 2 meines siebten Tätigkeitsberichts habe ich bereits auf mögliche, für den Betroffenen u.U. nachteilige Folgen durch Melderegisterauskünfte hingewiesen.

Eine Reihe von Fällen, in denen sowohl Behörden als auch Inkassobüros insbesondere aufgrund von automatisiert erteilten Melderegisterauskünften finanzielle oder sonstige Forderungen gegenüber völlig Unbeteiligten geltend machten, haben mich veranlaßt, im Einzelfall zu empfehlen, daß

1. eine Auskunftssperre im Datensatz der Betroffenen verfügt wurde und

2. von den beteiligten Stellen alle die Personenverwechslung betreffenden Unterlagen bereinigt wurden.

Darüber hinaus wurde unter Beteiligung meiner Geschäftsstelle das automatisierte Auskunftsverfahren einer Großstadt inzwischen modifiziert. Durch eindeutige Hinweise auf mögliche Personenverwechslungen oder durch aufklärende Hinweise vor Auskunftserteilung (z.B. Nachfragen nach weiteren identifizierenden Angaben beim Auskunftssuchenden, wenn mehr als eine Person gleichen Namens im Melderegister gefunden wird) wird den schutzwürdigen Belangen der Betroffenen so weit wie möglich Rechnung getragen. Seit dem Einsatz des verbesserten Auskunftsverfahrens im Sommer 1987 sind bei mir keine Beschwerden mehr über Personenverwechslungen eingegangen.

8.2. Veröffentlichung des Zuzugs von Neubürgern im kommunalen Mitteilungsblatt

Im Mitteilungsblatt einer Verwaltungsgemeinschaft wurden unter der Rubrik „Wir begrüßen zugezogene Mitbürger" Namen und Vornamen, akad. Grad und Wohnanschrift neuer Gemeindebürger einschließlich der mitzuziehenden Kinder veröffentlicht. Doch beileibe nicht alle Neubürger verspüren ein so ausgeprägtes Integrationsbedürfnis, daß ihre Ankunft der Allgemeinheit bekannt gemacht werden soll. Das Meldegesetz erlaubt eine solche Veröffentlichung nicht. Sie setzt vielmehr die vorherige Einwilligung der Betroffenen voraus.

Auf meine Beanstandung hin werden die Adressen von Zuziehenden nur noch nach schriftlicher Einwilligung veröffentlicht.

8.3. Auskunftsersuchen einer Krankenkasse zu Werbezwecken

Verschiedene Geschäftsstellen einer öffentlichen Krankenversicherung haben sich unter Berufung auf die für die Sozialleistungsträger einschlägigen Amtshilfebestimmungen (§§ 3 – 7 SGB X) an die Meldebehörden gewandt und um Auskunft über die genaue Wohnanschrift aus dem Melderegister über angebliche Kassen-Mitglieder gebeten. Nachgefragt wurde jeweils nach Angehörigen eines Geburtsjahrgangs, was vermuten ließ, daß es sich um Daten von Schulabgängern handelte (die vermutlich aus Schuljahresberichten entnommen waren und durch die Meldebehörde ergänzt werden sollten), nicht um Daten von Kassen-Mitgliedern.

Durch den von mir eingeschalteten und für die Kontrolle dieser Krankenkasse zuständigen Bundesbeauftragten für den Datenschutz wurde dies bestätigt. Die Auskunftsersuchen sollten der Mitgliederwerbung dienen. Die Geschäftsstellen der Krankenkasse wurden vom Bundesbeauftragten aufgefordert, solche Auskunftsersuchen nicht mehr im Rahmen der Amtshilfe an die Meldebehörden zu richten.

In diesem Zusammenhang sei darauf hingewiesen, daß das Bundesversicherungsamt mit Rundschreiben vom 24.5.1983 den Trägern der gesetzlichen Krankenversicherung sog. Wettbewerbsgrundsätze zur Beachtung mitgeteilt hat. U.a. ist es danach unzulässig, Adressenmaterial für Aufklärung und Werbung zu verwenden, bei dem die Möglichkeit besteht, daß es unter Verstoß gegen Datenschutzbestimmungen erlangt oder weitergegeben wurde. In dem Rundschreiben wird ferner darauf hingewiesen, daß Krankenkassen/Ersatzkassen mit ihrer Aufklärung und Werbung am Wettbewerb teilnehmen und damit privaten Unternehmen gleichzusetzen sind. Aus diesem Grunde halte ich hier eine Auskunftsverweigerung der bayerischen Meldebehörden für gerechtfertigt und geboten.

8.4. Melderegisterauskünfte an politische Parteien und Wählergruppen durch ein Service-Rechenzentrum

In früheren Tätigkeitsberichten habe ich wiederholt auf Probleme im Zusammenhang mit Melderegisterauskünften an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung hingewiesen.

Ein Vorfall vor der Bundestagswahl 1987 veranlaßt mich, nochmals dieses Thema aufzugreifen: Ein Bürgermeister hatte sich darüber beklagt, daß die Einwohnerdaten, die von dem Rechenzentrum im Auftrag der Gemeinde gespeichert werden, zu Unrecht an eine Partei weitergeleitet worden seien.

Das Bayer. Meldegesetz (MeldeG) regelt hier klar und eindeutig, daß nach Art. 35 Abs. 1 die Meldebehörde den Parteien und Wählergruppen im Zusammenhang mit allgemeinen Wahlen und Abstimmungen in den sechs der Stimmabgabe vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Nachnamen, akad. Grad und Wohnanschrift von Gruppen von Wahlberechtigten erteilen darf, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Jeder betroffene Wahlberechtigte hat das Recht, ohne Nennung von Gründen, der Weitergabe seiner Daten zu widersprechen.

Benötigen nun politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung im Rahmen des Art. 35 Abs. 1 MeldeG Wähleranschriften bayerischer Gemeinden, so setzen sie sich der Einfachheit halber unmittelbar mit der AKDB in Verbindung. Die AKDB hat sich zu diesem Zweck seit jeher von den Gemeinden entsprechende Zustimmungen bzw. Aufträge zur Datenweitergabe geben lassen.

Für die Bundestagswahl 1987 bot die AKDB ihren Anwendern zusätzlich die Möglichkeit, durch Eingabe eines bestimmten Auftrags in das DV-System der AKDB selbst zu bestimmen, ob Einverständnis mit Datenübermittlungen an Parteien im Rahmen des Art. 35 Abs. 1 MeldeG besteht. Der 1. Bürgermeister der Gemeinde, der generell keine Datenweitergabe an politische Parteien zum Zwecke der Wahlwerbung wünschte, ordnete gemeindeintern an, daß Einwohnerdaten an Parteien nicht weitergegeben werden sollen. Die AKDB gab gleichwohl Wähleranschriften aus der Gemeinde unter Berufung auf eine früher erteilte Zustimmung an eine Partei weiter.

Ich habe den Vorfall untersucht und bin zu dem Ergebnis gelangt, daß die Übermittlung von Wähleranschriften aus dieser Gemeinde durch die AKDB an die Partei zulässig war. Der Sachverhalt stellte sich für mich folgendermaßen dar:

Die Gemeinde hatte 1980 als „Herr der Daten" der Weitergabe der Adressen von Wahlberechtigten an im Bundestag vertretene Parteien auch für künftige Wahlen gegenüber der AKDB (Auftragnehmer) bis auf Widerruf schriftlich zugestimmt. Ein Widerruf dieser Zustimmung war nicht nachweisbar.

Nicht näher untersucht wurde, ob der Widerruf ein Geschäft der laufenden Verwaltung oder ein sog. Eilgeschäft war. Es war auch nicht zu entscheiden, ob der 1. Bürgermeister bei seiner Anordnung rechtsfehlerfrei gehandelt hat.

Auch ein Schreiben der AKDB an die angeschlossenen Meldebehörden, in dem auf die Möglichkeit hingewiesen wurde, den Auftrag „Weitergabe von Einwohnerdaten an Parteien" unmittelbar einzugeben, konnte die frühere Zustimmung der Gemeinde nicht unwirksam machen. Das Schreiben war nicht eindeutig dahin zu verstehen, daß die AKDB frühere Zustimmungen als gegenstandslos betrachten würde. Dem Schreiben durfte die Gemeinde daher nicht entnehmen, daß die AKDB von der Zustimmung aus dem Jahr 1980 keinen Gebrauch mehr machen würde.

Da die Gemeinde 1980 die Zustimmung zur Datenübermittlung an politische Parteien auch für künftige Wahlen erteilt hatte, konnte sie sich angesichts der Formulierung des Schreibens der AKDB nicht darauf verlassen, daß allein durch Nichtweitergabe einer klaren Weisung bzw. durch Nichteingabe des Kennzeichens die Übermittlung der Einwohneradressen unterbleiben würde. Die Gemeinde hätte vielmehr für klare Weisungen gegenüber ihrer Auftragnehmerin, der AKDB, sorgen müssen. Die Gemeinde hat sich zwar um den Nachweis dieser Weisung bemüht, ihn aber – wie oben ausgeführt – nicht erbringen können.

Gegenüber der AKDB und der Gemeinde habe ich allerdings deutlich gemacht, daß gerade im Hinblick auf den Datenschutz die Auftragslage der Gemeinde bei der AKDB jederzeit klar und überschaubar sein muß. Nur dann ist die Gemeinde wirklich „Herrin der Daten". Die Verantwortung hierfür trifft die AKDB in gleicher Weise wie die Gemeinden. Deshalb habe ich es begrüßt, daß die AKDB im Juni 1987 in diesem Punkt für klare Verhältnisse gesorgt hat. Ich habe

der AKDB auch nahegelegt, eine solche Dokumentation der aktuellen Auftragslage von Zeit zu Zeit zu wiederholen.

8.5. Alters- und Ehejubiläen

Aufgrund von Bürgeranfragen hatte ich mich erneut mit der Frage zu befassen, unter welcher Voraussetzung die Meldebehörde die Namen von Alters- und Ehejubilaren bekanntgeben darf.

a) Übermittlung von Alters- und Ehejubiläumsdaten an Parteien und Wählergruppen, Mitglieder parlamentarischer Vertretungskörperschaften und Bewerber für diese sowie an Presse und Rundfunk

An diese Empfänger darf die Meldebehörde nach Art. 35 Abs. 2 des Bayer. Meldegesetzes (MeldeG) Auskunft über Vor- und Familiennamen, akad. Grad, Wohnanschrift sowie Tag und Art des Jubiläums erteilen. Die Auskunft liegt im pflichtgemäßen Ermessen der Gemeinde.

Die Betroffenen haben die Möglichkeit, der Weitergabe ihrer Jubiläumsdaten ohne Nennung von Gründen zu widersprechen. Auf dieses Widerspruchsrecht sind sie bei ihrer Anmeldung hinzuweisen.

Diese gesetzliche Regelung hat zur Folge, daß diejenigen Bürger, die schon vor Inkrafttreten des Meldegesetzes am 1.4.1983 in einer Gemeinde gemeldet waren (und seither nicht umgezogen sind), in aller Regel nichts von ihrem Widerspruchsrecht wissen und sich im Einzelfall z.B. durch eine Veröffentlichung ihres Jubiläums in der Presse oder im Rundfunk in ihren schutzwürdigen Belangen beeinträchtigt fühlen können.

Im Interesse einer bürgerfreundlichen Verwaltung wäre zu wünschen, daß die Meldebehörden von Zeit zu Zeit in ortsüblicher Weise auf die vom Meldegesetz vorgesehenen Widerspruchsrechte hinweisen würden.

b) Übermittlung von Alters- und Ehejubiläumsdaten an den Bayerischen Ministerpräsidenten, den Landrat und den Bürgermeister

Auf der Grundlage von Art. 31 MeldeG sehen § 10 der Bayer. Meldedatenübermittlungsverordnung und die Vollzugsbekanntmachung zum Meldegesetz die Übermittlung von Daten über Alters- und Ehejubiläen an den Bayerischen Ministerpräsidenten, an den Landrat sowie an den Bürgermeister vor. Es gehört zur rechtmäßigen Aufgabenerfüllung dieser Amtsträger, Jubilaren zu gratulieren. Nach Art. 35 Abs. 2 MeldG eingelegte Widersprüche wirken hier nicht.

c) Übermittlung von Jubiläumsdaten an den Ortspfarrer

Immer wieder wird gefragt, ob die Meldebehörde dem Ortspfarrer Auskünfte über Alters- und Ehejubilare erteilen darf. Hierzu ist zu bemerken, daß der Empfängerkatalog des Art. 35 Abs. 2 MeldeG die Vertreter öffentlich-rechtlicher Religionsgesellschaften nicht enthält. Jubiläumsauskünfte der Meldebehörde scheiden deshalb nach dieser Bestimmung aus.

Allerdings können die öffentlich-rechtlichen Religionsgesellschaften nach Art. 32 Abs. 1 und 2 MeldeG die dort aufgezählten Einwohnerdaten – also u.a. auch das Geburtsdatum – zur Erfüllung ihrer Aufgaben (dazu zählen auch seelsorgerische, caritative, soziale und kulturelle Aufgaben) erhalten. Gegen die Übermittlung von Altersjubiläumsdaten der Kirchenmitglieder an den Ortspfarrer bestehen somit keine Bedenken.

Nach Art. 32 MeldeG dürfen dem Ortspfarrer jedoch keine **Ehe**jubiläumsdaten übermittelt werden, da diese Vorschrift eine abschließende Regelung darstellt.

Um eine Veröffentlichung der Jubiläumsdaten z.B. im Kirchenblatt in solchen Fällen zu vermeiden, in denen nach Art. 35 Abs. 2 MeldeG Widersprüche eingelegt wurden, sollten sich die Meldebehörden mit den Ortspfarrern dahin verständigen, daß sie ihnen zu Veröffentlichungszwecken nur die Jubiläumsdaten von Personen übermitteln, die von ihrem Widerspruchsrecht (für den weltlichen Bereich) keinen Gebrauch gemacht haben. Ebenso sollte verhindert werden, daß nach Art. 34 Abs. 5 und Abs. 7 MeldeG gesperrte Daten über die Pfarreien an die Öffentlichkeit gelangen (Sperre wegen Gefahr für Leib und Leben etc. sowie bei Adoptionssperren). Nach meinen Erfahrungen haben die Ortspfarrer in aller Regel für eine solche Absprache Verständnis.

Im übrigen habe ich bei den Datenschutzbeauftragten der Katholischen und Evangelischen Kirche eine Angleichung des kirchlichen Datenschutzrechts an das weltliche Datenschutz- bzw. Melderecht angeregt. Dieser Anregung wurde zwischenzeitlich entsprochen.

8.6. Übermittlung von Meldedaten an Adreßbuchverlage

Im fünften Tätigkeitsbericht habe ich den Meldebehörden empfohlen, ihre Gemeindebürger auf eine beabsichtigte Meldedatenübermittlung an Adreßbuchverlage und auf das in Art. 35 Abs. 3 des Meldegesetzes vorgesehene Widerspruchsrecht ortsüblich hinzuweisen. Nicht jeder möchte sich im örtlichen Adreßbuch wiederfinden.

In der Vollzugsbekanntmachung zum Meldegesetz wird diese Empfehlung ebenfalls gegeben. Sie wird in der Praxis allerdings nicht immer befolgt. So mußte ich in einer Reihe von Fällen nicht informierte Bürger für die Zukunft auf die vom Meldegesetz vorgesehenen Widerspruchsrechte verweisen.

Aus Gründen der Bürgerfreundlichkeit rege ich nochmals an, die Bürger von Zeit zu Zeit in ortsüblicher Weise über ihre Widerspruchsrechte nach dem Meldegesetz zu informieren.

8.7. Übermittlung von Daten Deutscher, die auch eine fremde Staatsangehörigkeit besitzen, an Ausländerbehörden

Die regelmäßige Übermittlung von Daten Deutscher, die zugleich eine fremde Staatsangehörigkeit besitzen, durch Melde- an Ausländerbehörden war vom Landesbeauftragten in der Vergangenheit für bedenklich erachtet worden, da nicht erkennbar schien, zu welchem Zweck diese Daten bei Ausländerämtern gesammelt werden.

Gegen die Regelung in der Meldedatenübermittlungs-Verordnung, die diese Datenübermittlung vorschreibt, haben in der Folgezeit Betroffene Popularklage beim Bayerischen Verfassungsgerichtshof erhoben. Das Gericht wies nun die Klage ab und stellte fest, die Regelung verstoße nicht gegen Normen der Bayerischen Verfassung. Das Sammeln der eingehenden Meldungen werde in § 27 des Ausländergeset-

zes geregelt. Als Bundesrecht sei § 27 nicht Gegenstand der Entscheidung. Aus der Begründung des Urteils ist zu entnehmen, daß in dem Verfahren auch nicht zu prüfen war, unter welchen Voraussetzungen die Ausländerbehörde ihrerseits etwa befugt wäre, andere Stellen von der weiteren Staatsangehörigkeit eines Deutschen zu unterrichten.

Der Verfassungsgerichtshof weist in der Begründung darauf hin, daß sich aus dem Recht auf informationelle Selbstbestimmung Schranken für die Weitergabe der Meldung der weiteren Staatsangehörigkeiten von der Ausländerbehörde an andere Stellen ergeben könnten, daß in der Entscheidung jedoch nicht darauf eingegangen zu werden brauchte, ob und gegebenenfalls welche ergänzenden Regelungen der Gesetzgeber insoweit zu treffen haben werde. Im Popularklageverfahren genüge die Feststellung, daß das bloße Sammeln der entsprechenden Mitteilung eine Aufgabe der Ausländerbehörde sei, die in einer Verwaltungsvorschrift zur Durchführung des § 27 des Ausländergesetzes eine ausreichende Grundlage finde.

8.8. Online-Zugriff auf Melderegisterdaten – Berücksichtigung des Grundsatzes der Erforderlichkeit

Mit fortschreitender Automation – auch im Kommunalbereich – werden in den einzelnen Fachabteilungen der Gemeinden zunehmend Bildschirmarbeitsplätze eingerichtet, die es den Benutzern ermöglichen, direkt (online) auf das Melderegister zuzugreifen, sei es um Arbeitsabläufe zu optimieren, sei es aus Gründen der Bürgerfreundlichkeit. Voraussetzung für diesen Direktzugriff ist, daß dem (befugten) Benutzer nur die Informationen aus dem Melderegister auf den Bildschirm übertragen werden, die für dessen rechtmäßige Aufgabenerfüllung erforderlich sind (vgl. Art. 31 Abs. 1 und Abs. 7 des Meldegesetzes – MeldeG). Die Steuerung bzw. Festlegung, welche Melderegisterdaten auf welchem Bildschirm erscheinen dürfen, erfolgt per Programm. Die Daten, die für die rechtmäßige Aufgabenerfüllung des Sachbearbeiters erforderlich sind, werden in sogenannten Bildschirmmasken sichtbar gemacht.

Meinen Feststellungen zufolge wird der Grundsatz der Erforderlichkeit bei der Verwendung der Bildschirmmasken nicht immer ausreichend beachtet. So konnte ich eine Stadt davon überzeugen, daß die Maskeninhalte, die den einzelnen Fachabteilungen zur Verfügung stehen, generell zu überprüfen und zu reduzieren waren. Ein endgültiges Ergebnis steht allerdings noch aus.

Nach meinen Erkenntnissen wird das Bildschirm-Maskenangebot der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) von verschiedenen Gemeinden nicht immer korrekt eingesetzt. Die AKDB bietet als Service-Rechenzentrum für zahlreiche kommunale Anwender eine Palette gängiger Bildschirmmasken an, die erfahrungsgemäß geeignet sind, die Anforderungen kommunaler Aufgabenbereiche abzudecken. Es liegt jedoch einzig in der Verantwortung der Kommune als „speichernde Stelle" bzw. als „Herrin der Daten", den einzelnen Fachabteilungen über die Bildschirmmasken jeweils nur die wirklich erforderlichen Daten zur Verfügung zu stellen. Lassen sich verfügbare Masken nicht auf das tatsächlich erforderliche Maß begrenzen, dürfen sie nicht verwendet werden. Da die AKDB als Auftragnehmer die Verarbeitung personenbezogener Daten nach der jeweiligen Weisung der Gemeinde durchzuführen hat, sind die betroffenen Gemeinden aufgefordert, entsprechende datenschutzgerechte Bildschirmmasken zu verlangen oder auf den Einsatz von Masken zu verzichten, wenn damit mehr Daten übermittelt würden, als zur rechtmäßigen Aufgabenerfüllung erforderlich ist.

8.9. Anpassung der Datensätze für das Meldewesen an das Melderecht

Obgleich das Meldegesetz am 1.4.1983 in Kraft getreten ist und Art. 43 Abs. 1 die Anpassung des Melderechts bis 31.12.1984 verlangte, zieht sich die Umstellung der Datensätze wegen der Komplexität der automatisierten Einwohnerverfahren teilweise bis zum heutigen Tage hin. Auch vier Jahre danach stelle ich gelegentlich noch Datenfelder in Melde-Datensätzen fest, die vom neuen Melderecht nicht vorgesehen sind und deren Speicherung daher unzulässig ist.

Allerdings kann bei den zentral entwickelten Einwohnerverfahren, wie sie von der AKDB für eine Vielzahl bayerischer Gemeinden, aber auch von größeren Städten eingesetzt werden, nach der bisherigen Erfahrung von einer weitgehenden Übereinstimmung der Datenverarbeitung mit dem Melderecht ausgegangen werden. Rechts- und sachkundiges Personal ist schließlich an der Entwicklung und Fortschreibung dieser Verfahren beteiligt. Nicht zuletzt deshalb geht Art. 36 Abs. 1 des Meldegesetzes davon aus, daß sich die Meldebehörden zur automatisierten Abwicklung des Meldewesens der AKDB bedienen können, die auch gemäß Nr. 3.7 der Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz als „sorgfältig ausgewählt" – also als Garant für eine rechtmäßige (Auftrags-)Datenverarbeitung gilt.

Gesteigerter Beachtung bedürfen jedoch die DV-Verfahren des Einwohnerwesens, die den Gemeinden in zunehmendem Maße von privaten Unternehmen angeboten werden. Auch wenn sich Gemeinden im Vertrauen auf eine zugesicherte Gesetzeskonformität der ADV-Verfahren privater Anbieter bedienen, müssen diese Programme in eigener Verantwortung überprüft und datenschutzrechtlich freigegeben werden (Art. 26 Abs. 1, 2 und 4 BayDSG).

Zur Durchsetzung und Einhaltung der gesetzlichen Datenschutzbestimmungen werde ich im Bereich der Melderegisterführung meine Kontrolltätigkeit in naher Zukunft erheblich verstärken.

8.10. Kennzeichnung von Einwohnern als Wohngeldempfänger im Meldedatensatz

Eine kreisfreie Stadt beabsichtigte die Einführung eines automatisierten Verfahrens, das es der Wohngeldstelle ermöglichen sollte, im automatisiert geführten Datenbestand der Meldebehörde zu kennzeichnen, wer Wohngeldempfänger ist. Aufgrund dieses Kennzeichens sollten regelmäßig (z.B. 1 mal monatlich) Listen über die wohngeldbeziehenden Personen ausgedruckt werden, die entweder verzogen oder verstorben sind. Die vorgesehene Übermittlung der verstorbenen und weggezogenen Wohngeldbezieher an die Wohngeldstelle ist grundsätzlich zulässig. Fraglich war jedoch, ob der Meldedatensatz physisch um das Merkmal „Wohngeldempfänger" erweitert werden durfte. Hierzu habe ich mich wie folgt geäußert:

Auch wenn durch technisch-organisatorische Maßnahmen sichergestellt würde, daß außer der Wohngeldstelle weder das Einwohneramt noch eine andere Stelle, die Zugriff auf das Melderegister hat, Kenntnis von dem Kennzeichen „Wohngeldempfänger" nehmen kann, hat der Gesetzgeber eine solche Möglichkeit zur Erweiterung des Melderegisters um Kennzeichen für andere Fachgebiete der Verwaltung in Art. 3 des Bayer. Meldegesetzes nicht vorgesehen. Um keinen Präzedenzfall zu schaffen, möchte ich von diesem Vorhaben dringend abraten. Sie würde zu einer tatsächlichen (physischen) Erweiterung des Melderegisters führen, die der abschließenden Festlegung des Inhalts des Melderegisters zuwiderliefe und wäre ein Schritt in Richtung auf ein erweitertes Meldewesen als allgemeine Informationssammlung für eine Vielzahl von Verwaltungszweigen – ein Schritt, der bei Schaffung des neuen Melderechts, im Gegensatz zu früheren Plänen, aus guten Gründen unterblieb.

Die Stadt akzeptierte dieses Argument und baut nun eine eigene Wohngeldatei auf. Sie speichert darin auch das Ordnungsmerkmal des Melderegisters. Anhand des Ordnungsmerkmals soll regelmäßig ein Datenabgleich mit dem Melderegister zur Feststellung vorgenommen werden, ob der Wohngeldempfänger noch gemeldet bzw. verzogen oder verstorben ist.

8.11. Auskunftspflicht des Meldepflichtigen – Nachweis der Angaben

In einer Beschwerde wurde bemängelt, daß sich eine Meldebehörde zum Nachweis der Richtigkeit der Angaben des Meldepflichtigen u.a. das gesamte Scheidungsurteil abgelichtet und zu den Meldeunterlagen genommen hat.

Das Ablichten von Nachweisen und Unterlagen, die die Richtigkeit der Angaben auf dem Meldeschein und im Melderegister (hier: Angabe zum Familienstand) bestätigen, ist im Rahmen des Art. 19 MeldeG i.V.m. Nr. 19 der Vollzugsbekanntmachung zulässig, soweit die Informationen zur melderechtlichen Aufgabenerfüllung erforderlich sind. Deshalb habe ich keine Einwände, wenn sich die Meldebehörde als Nachweis für die Scheidung den einschlägigen Teil des Urteiltenors ablichtet.

8.12. Auskünfte aus dem Melderegister an die gemeindliche Steuerstelle

Eine Gemeinde bat um Stellungnahme zu der Frage, ob die gemeindliche Steuerstelle aus dem Melderegister personenbezogene Daten (Namen und Anschrift) von Personen, die von der Grundsteuer befreit sind, erhalten könne. Die Steuerstelle möchte auf diese Weise Erkenntnisse darüber gewinnen, ob die Voraussetzungen für die Grundsteuerbefreiung bei den Anwesen bzw. Personen, die mit Bescheid des Landratsamtes von der Grundsteuer auf 10 Jahre befreit sind, noch vorliegen.

Die Bescheide des Landratsamts über die Grundsteuerbefreiung sind für die Gemeinde bindend. Die Gemeinden sind jedoch gehalten, Erkenntnisse, die z.B. den Widerruf der Anerkennung als steuerbegünstigte Wohnung oder den Wegfall der Grundsteuervergünstigung bei öffentlich geförderten Wohnungen zur Folge haben können, dem Landratsamt mitzuteilen. Die Grundsteuererhebung kann als Aufgabe im Sinne von Art. 31 Abs. 1 und 7 des Bayer. Meldegesetzes betrachtet werden, zu deren Erfüllung das gemeindliche Meldeamt die erforderlichen Daten zur Verfügung stellen muß. Allerdings muß darauf geachtet werden, daß die gemeindliche Steuerstelle nur Meldedaten über steuerbegünstigte Wohnungen erhält, nicht sämtliche Änderungen des Melderegisters.

9. Steuerverwaltung

Steuerdatenabrufverordnung (StDAV)

Der Bundesminister der Finanzen bereitet unter Beteiligung der Länder eine Verordnung über den automatisierten Abruf von Steuerdaten vor, die beim Bundesamt für Finanzen, den Finanzämtern und den Gemeinden gespeichert sind. Das Bayer. Staatsministerium der Finanzen hat mich über den derzeitigen Entwurfsstand unterrichtet und mitgeteilt, daß derzeit noch die Frage strittig sei, ob auch Oberbehörden eine Zugriffsberechtigung auf Steuerdaten erhalten sollen. Aus seiner Sicht sollten weder Oberfinanzdirektionen noch oberste Finanzbehörden eine Zugriffsberechtigung erhalten.

Diese Forderung des Finanzministeriums, die den Anliegen des Datenschutzes entspricht, unterstütze ich nachdrücklich. Für einen unmittelbaren Zugriff der Oberbehörden auf Steuerdaten in den Datensammlungen der Finanzverwaltung besteht keine Notwendigkeit. Dann ist es aber auch notwendig, zur Begrenzung des Kreises der Zugriffsberechtigten im Interesse des Datenschutzes, den Oberbehörden keine unmittelbaren Zugriffsrechte einzuräumen.

10. Personalwesen

10.1. Einsichtnahme der Frauenbeauftragten in Personalunterlagen

Eine Stadt mußte klären, unter welcher Voraussetzung die Frauenbeauftragte Einsicht in Personalunterlagen erhalten könne. Sie bat den Landesbeauftragten für den Datenschutz um Äußerung.

Ich habe hierzu Stellungnahmen der Staatsministerien für Arbeit und Sozialordnung – Leitstelle für die Gleichstellung der Frauen – sowie des Innern und der Finanzen eingeholt. Alle Stellungnahmen wiesen auf das Erfordernis der Einwilligung des Betroffenen hin. Das Staatsministerium der Finanzen führte aus:

„Die Einsichtnahme durch die Frauenbeauftragte dient, seiner Aufgabe entsprechend, dem Zweck, Mitarbeiterinnen in Fragen der Gleichstellung zu unterstützen. Sie ist der Einsicht des Personalrates in Personalakten ähnlich. Auch gem. Art. 69 Abs. 3 Satz 4 BayPVG dürfen Personalakten nur mit schriftlicher Zustimmung des Beschäftigten und nur von einem von ihm bestimmten Mitglied des Personalrats eingesehen werden. Ein weitergehendes Einsichtsrecht ohne Zustimmung des Betroffenen kann auch einer Frauenbeauftragten nicht zugestanden werden. Abweichungen vom Grundsatz der Geheimhaltung zugunsten der Frauenbeauftragten müssen wohl als rechtswidrig angesehen werden."

Ich habe mich dieser Auffassung angeschlossen.

10.2. Versendung eines Wählerbriefes an dienstliche Anschriften

Vor der Landtagswahl 1986 hat ein Abgeordneter des Bayerischen Landtags, der vorher im Staatsministerium des Innern Sachgebietsleiter im Polizeibereich war, einen Wählerbrief an Bedienstete verschiedener Behörden unter deren dienstlicher Anschrift versandt. In mehreren Eingaben von Behördenangehörigen wurde der Landesbeauftragte um Überprüfung gebeten, ob die dienstlichen Anschriften unter Verstoß gegen datenschutzrechtliche Vorschriften erlangt worden waren.

Die umfangreichen Überprüfungen dieser Angelegenheit durch das Bayer. Staatsministerium des Innern und den Landesbeauftragten für den Datenschutz haben ergeben, daß für die Beschaffung des Adreßmaterials, das zur Beschriftung der Wählerbriefe erforderlich war, keine Dateien und Datenverarbeitungsanlagen der bayerischen Polizei oder anderer staatlichen Stellen verwendet worden sind. Der Verdacht, der Abgeordnete habe sich als ehemaliger Sachgebietsleiter im Bayer. Staatsministerium des Innern das Adreßmaterial auf diese Weise beschafft, ist nach meinen Ermittlungen unbegründet. Frühere Mitarbeiter des Abgeordneten haben erklärt, daß sie zu keinem Zeitpunkt zur Beschaffung von Adressenmaterial aus den ihnen zugänglichen Datenverarbeitungsanlagen behilflich waren.

Neben meinen Ermittlungen im Bayer. Staatsministerium des Innern habe ich auch Nachforschungen beim Bayer. Landeskriminalamt als zentraler Stelle für die polizeiliche Datenverarbeitung durchgeführt. Nach meinen Feststellungen ist es ausgeschlossen, daß für die Adressenbeschaffung Datenverarbeitungsanlagen des Bayer. Landeskriminalamtes verwendet worden sind. So waren beispielsweise die verwendeten Adressen im Gegensatz zu den beim Bayer. Landeskriminalamt geführten Datenbeständen nicht aktualisiert. Wäre die EDV-Anlage des Landeskriminalamts verwendet worden, hätte es – wie dies der Fall war – auf den Wählerbriefen keine fehlerhaften Adressen gegeben. Außerdem haben die zuständigen Beamten glaubhaft versichert, dem Abgeordneten keine Adressen beschafft zu haben. Zum gleichen Ergebnis kamen meine Nachforschungen beim Polizeipräsidium München.

Nach den Angaben des Abgeordneten wurden die vorgedruckten Schreiben an befreundete Kollegen ausgehändigt, die ihrerseits die Schreiben mit Anschriften versahen.

Die Angaben des Abgeordneten sind plausibel und nicht widerlegbar. So weisen mir überlassene Wählerbriefe im Adressenfeld verschiedene Schriftbilder auf, die von Schreib- und Speicherschreibmaschinen bzw. von auf dem Markt erhältlichen Druckern stammen können. Eine Verletzung datenschutzrechtlicher Vorschriften war somit nicht festzustellen.

11. Statistik

11.1. Volkszählung 1987

Der Landesbeauftragte war von Anfang an in die Vorbereitung der Volkszählung eingeschaltet. Er hat es als seine vorrangige Aufgabe angesehen, durch intensive Beratung und Kontrolle der mit der Vokszählung befaßten Behörden die sorgfältige, peinlich genaue Einhaltung der im Volkszählungsgesetz 1987 normierten Vorschriften sicherzustellen und so Mißtrauen und Ängsten den Boden zu entziehen. Auch bei der Durchführung und Auswertung der Volkszählung war und ist er beteiligt und in diesem Sinn tätig. Die Staatsregierung hat am 19. Mai 1987 noch einmal ausdrücklich bekräftigt: „Die Volkszählung unterliegt nach geltendem Recht in allen ihren Phasen der Kontrolle des Landesbeauftragten für den Datenschutz."

Ich habe bisher von den bayerischen Behörden jede erbetene Unterstützung erhalten. Meine Forderungen wurden erfüllt. Wünschen und Anregungen wurde soweit wie möglich entsprochen.

Die Überwachung der Volkszählung durch den Landesbeauftragten setzte in Bayern bereits bei den Erstarbeiten für den Entwurf einer Verordnung zur Durchführung des Volkszählungsgesetzes 1987 (DV VZG) ein. Der Bundesgesetzgeber hatte es den Ländern überlassen, die Erhebungsstellen zu bestimmen und das Nähere zur Sicherstellung des räumlichen, organisatorischen und personellen Abschottungsgebotes, einer Kernforderung des Datenschutzes bei statistischen Erhebungen, zu regeln.

Das Landesamt für Statistik und Datenverarbeitung, das das Erhebungsverfahren, den Termin- und Ablaufplan sowie die Geheimhaltung durch technische und organisatorische Verwaltungsvorschriften zu regeln hatte, stimmte diese mit dem Landesbeauftragten ab. Damit beim praktischen Vollzug dieser Großerhebung das Grundrecht auf informationelle Selbstbestimmung gewahrt blieb, wurden vom Landesbeauftragten folgende Forderungen erhoben und vom Staatsministerium des Innern sowie vom Landesamt für Statistik und Datenverarbeitung verwirklicht:

- Die Räume der Erhebungsstelle dürfen nur für die Durchführung der Volkszählung genutzt werden. In ihnen dürfen keine sonstigen Verwaltungsvorgänge der Gemeinde/Verwaltungsgemeinschaft lagern.
- Alle Verwaltungabläufe der Erhebungsstelle müssen innerhalb ihrer Organisation abgewickelt werden (z.B. eigene Arbeitskräfte, kein Anschluß an eine zentrale Schreibkanzlei).
- Festlegung von Inhalt und Umfang der Kontrollen der getroffenen Sicherungsmaßnahmen und der dafür verantwortlichen Personen.
- Ein mehrmaliger Wechsel eines Mitarbeiters zwischen Erhebungsstelle und übriger Verwaltung muß ausgeschlossen sein.
- Die in den örtlichen Erhebungsstellen tätigen Personen dürfen, soweit sie statistische Einzelangaben in den Erhebungsvordrucken bearbeiten, nicht gleichzeitig mit anderen Aufgaben des Verwaltungsvollzugs betraut werden.
- Beim Reinigungspersonal sollte unterschieden werden, ob es sich um eigenes oder fremdes Personal handelt. Bei Fremdpersonal sollte die Reinigung in jedem Fall unter besonderer Aufsicht erfolgen.

Die Beratung und Kontrolle des Landesbeauftragten umfaßte den staatlichen sowie den kommunalen Bereich. Die Großstädte, aber auch andere Gemeinden stimmten die

Dienstanweisung, in der die Volkszählungsräume, die Aufgabenverteilung, der Arbeitsablauf und die Sicherungsmaßnahmen festgelegt waren, mit mir ab.

11.1.1. Beratung und Kontrolle in der Vorbereitungsphase

a) Besuche bei Gemeinden, Städten und Landratsämtern

Zahlreiche Besuche, beginnend im Frühjahr 1986, dienten dazu, die Landratsämter sowie ausgewählte Gemeinden bei der Einrichtung der Erhebungsstellen zu beraten.

- Nach dem Volkszählungsgesetz 1987 waren die Räume der Erhebungsstelle von der übrigen Verwaltung abzuschotten. Sie durften nur für die ihr zugewiesenen Verwaltungsaufgaben genutzt werden. Räumliche Abschottung erforderte jedoch nicht, daß die Erhebungsstelle grundsätzlich außerhalb des Rathauses oder eines anderen kommunalen Verwaltungsgebäudes untergebracht werden mußte, wie es in einigen Eingaben gefordert worden ist. Zwar haben viele Gemeinden für die Volkszählung zusätzliche Räume angemietet. Das lag aber daran, daß die Verwaltung ohnehin bereits in sehr beengten Verhältnissen arbeiten mußte und/oder keine den Anforderungen der Datensicherung entsprechenden Räumlichkeiten vorhanden waren.

- Die Erhebungsstelle war auch organisatorisch von der übrigen Verwaltung abzuschotten. Sie mußte eine eigene organisatorische Einheit bilden, die mit keinen anderen Verwaltungsaufgaben befaßt ist.

- Schließlich war die Erhebungsstelle personell abzuschotten: die hier tätigen Personen durften nicht mit anderen Verwaltungsaufgaben betraut werden. Der Bundesgesetzgeber war sich zwar bewußt, daß die strikte personelle Trennung kleinen Gemeinden Probleme bereiten würde. Er hielt diese Forderung aber für unverzichtbar, damit die vom Bundesverfassungsgericht als notwendig vorausgesetzte Akzeptanz der Zählung in der Bevölkerung gewährleistet war.

  aa) Im Mittelpunkt der Diskussion um die personelle Abschottung stand in der Vorbereitungsphase die Frage: Wer ist ein geeigneter Zählungsleiter? Da das personelle Abschottungsgebot den „ganzen Mann" erforderte, galt es, jemanden zu finden, der die nötige Qualifikation hatte, um das nicht einfache Zählgeschäft in einer Erhebungsstelle zu leiten, und der gleichzeitig von seinen bisherigen Aufgaben für 6 und mehr Wochen freigestellt werden konnte. Soweit dies nicht möglich war, fanden gerade kleine Gemeinden häufig vernünftige Lösungen: Vielfach wurde der pensionierte frühere geschäftsleitende Beamte der Gemeinde oder eine aus familiären Gründen beurlaubte Mitarbeiterin für die Volkszählung gewonnen.

  bb) Anlaß zu Zweifelsfällen war die im Volkszählungsgesetz 1987 nicht ausdrücklich geregelte Frage, ob – wie bei der Auswahl der Zähler nach § 10 VZG – ein Interessenkonflikt den Einsatz als Leiter oder Mitarbeiter der Erhebungsstelle ausschloß.

Das Staatsministerium des Innern, das Landesamt für Statistik und Datenverarbeitung, die Landratsämter und der Landesbeauftragte für den Datenschutz bemühten sich, daß die Gemeinden den Einsatz von Bediensteten aus sensiblen Verwaltungsbereichen in den Erhebungsstellen vermieden. Sobald ein Fall bekannt wurde, wurde der Bürgermeister auf die ungünstigen Auswirkungen hingewiesen, die der Einsatz eines solchen Mitarbeiters in der Erhebungsstelle auf die Akzeptanz der Volkszählung nicht nur in seiner Gemeinde, sondern im ganzen Land haben könnte.

Das Staatsministerium des Innern machte in diesen Fällen ausschließlich Akzeptanzgründe geltend. Ein Anlaß für eine rechtsaufsichtliche Weisung hingegen lag nach dortiger Auffassung nicht vor, da die Vermeidung von Interessenkonflikten in der Erhebungsstelle rechtlich nicht zwingend vorgeschrieben sei. § 10 des Volkszählungsgesetzes gelte ausschließlich für die Auswahl der Zähler, nicht aber für die Beschäftigten der Erhebungsstelle. Für diese habe der Gesetzgeber das Abschottungsgebot geschaffen. Auch eine Weisung im Rahmen der Fachaufsicht nach Art. 109 S. 2 Ziff. 1. Bayer. Gemeindeordnung war in den zu entscheidenden Fällen nach dortiger Auffassung nicht möglich, da weder das Gemeinwohl noch öffentlich rechtliche Ansprüche einzelner eine solche Weisung erforderten. Die Gemeinden und Landratsämter bestätigten, daß es in den betreffenden Gemeinden keinerlei Akzeptanzprobleme gebe.

Demgegenüber vertreten die Datenschutzbeauftragten und das Statistische Bundesamt die Auffassung, was für die Zähler gelte, müsse grundsätzlich erst recht für Leiter und Mitarbeiter der Erhebungsstelle gelten. Hauptgrund für die Aufhebung des Volkszählungsgesetzes 1983 war der vorgesehene Melderegisterabgleich, also die Verquickung von Melderechtsvollzug mit Statistik. Das Bundesverfassungsgericht hat dem Gesetzgeber aufgegeben, organisatorische und verfahrensrechtliche Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung zu treffen. Dies hat der Bundesgesetzgeber unter anderem durch die Vorschrift über die Abschottung der Erhebungsstelle von der Vollzugsverwaltung in § 9 Abs. 1 Volkszählungsgesetz 1987 verwirklicht. Das Bundesverfassungsgericht hat auch auf die hohe Bedeutung der Akzeptanz der Volkszählung hingewiesen, die ebenfalls durch klare organisatorische Trennung von Statistik und Verwaltung gesichert werden sollte. Eine solche klare Trennung hat mein Vorgänger als gefährdet angesehen, wenn beispielsweise Personal des Meldeamtes die Erhebungsstelle leite, bzw. dort tätig war.

cc) Manche Eingabenführer beklagten sich darüber, daß sie zur Volkszählung Briefe vom ersten Bürgermeister erhalten hätten. Diese Briefe waren nicht zu beanstanden.

§ 6 Abs. 1 DV-VZG bestimmt, daß der erste Bürgermeister Leiter der örtlichen Erhebungsstelle ist. Diese Festlegung verstößt nicht gegen Vorschriften des Datenschutzes. Die Bestimmung steht nicht in Widerspruch zum Abschottungsgebot des Volkszählungsgesetzes. Soweit der erste Bürgermeister einer Gemeinde von der Delegationsmöglichkeit des § 6 Satz 6 DV-VZG keinen Gebrauch macht, muß allerdings auch er für seine Person das Abschottungsgebot befolgen und darf keine anderen Verwaltungsaufgaben wahrnehmen.

b) Fragebogenaktion

Ein Besuch bei allen bayerischen Gemeinden war naturgemäß nicht möglich. Ich habe deshalb zusätzlich vor Beginn der Volkszählung an ausgewählte Gemeinden einen umfangreichen Fragebogen versandt, um stichprobenweise einen Überblick über die Einhaltung des Datenschutzes zu erhalten. Dieser Fragebogen wurde auch dann an Gemeinden und Erhebungsstellen gesandt, wenn Bürger dem Landesbeauftragten die Sorge vortrugen, bereits im organisatorischen Vorfeld läge in ihrer Gemeinde etwas im Argen, sei es, daß noch keine eigenen Räume für die Erhebungsstelle vorgesehen seien, sei es, daß der Zählleiter gleichzeitig seine normale Arbeit miterledigen solle. Auch soweit durch die Fragebogenaktion bekannt wurde, daß Bedienstete des Ordnungs-, Melde- und Sozialamtes sowie Mitarbeiter des gemeindlichen Versicherungsamtes als Zählungsleiter eingesetzt werden sollten, habe ich das Landesamt für Statistik und Datenverarbeitung als oberste Erhebungsstelle hierüber unterrichtet und um Abhilfe gebeten.

c) Datenschutz bei der Zählergewinnung

aa) Öffentliche Bedienstete als Zähler

Nach der Bekanntmachung der Bayer. Staatsregierung vom 4. November 1986 waren die Leiter der Behörden und Dienststellen des Freistaates Bayern auf Anforderung der Erhebungsstellen verpflichtet, die Namen, Anschriften, Dienststellen und beruflichen Tätigkeiten ihrer Bediensteten mitzuteilen. In Übereinstimmung mit dem Staatsministerium des Innern habe ich den Behörden und Dienststellen, die sich in diesem Zusammenhang an mich gewandt haben, empfohlen, wie folgt zu verfahren:

Die jeweilige Dienststelle sucht aus ihrem Mitarbeiterstamm bestimmte Personen aus, die nach dortiger Beurteilung als Zähler in Betracht kommen. Dabei ist zu berücksichtigen, daß § 10 Abs. 5 VZG verlangt, daß Zähler die Gewähr für Zuverlässigkeit und Verschwiegenheit bieten müssen. Sie dürfen nicht in der Nachbarschaft oder bei Vorliegen eines Interessenkonfliktes eingesetzt werden. Den danach ausgewählten Personen sollte freigestellt werden, ob sie am Dienstort oder am Wohnort eingesetzt werden wollen. Erst nach Klärung des Zählortes sollte die entsprechende Mitteilung an die Erhebungsstelle erfolgen.

bb) Dürfen andere öffentliche Stellen Anschriften zur Zählergewinnung übermitteln?

Schwierigkeiten bei der Zählergewinnung gab es vor allem in den großen Städten.

Eine Erhebungsstelle wandte sich daher an die Zusatzversorgungskasse der bayerischen Gemeinden mit der Bitte, im Rahmen der Amtshilfe die Anschriften der Personen, die eine Rente aus der Zusatzversicherung für Angestellte beziehen und früher bei der Stadtverwaltung beschäftigt waren, zu übermitteln. Personen, die älter als 70 Jahre sind oder außerhalb des Stadtgebietes wohnen, Witwen und Waisen sowie Personen, die über Zustelladressen erreichbar sind, sollten ausgenommen werden. Nach der Datenübermittlung sollten die ehemaligen Bediensteten von der Erhebungsstelle auf die Möglichkeit zur **freiwilligen** Mitarbeit als Zähler hingewiesen werden. In einem anderen Fall wandte sich eine Erhebungsstelle an eine Bezirksfinanzdirektion mit der Bitte, die Anschriften von Versorgungsempfängern mit den oben genannten Kriterien zu benennen.

Der Landesbeauftragte hat in beiden Fällen keine datenschutzrechtliche Bedenken geltend gemacht. Dabei ging er von folgender Überlegung aus:

Die Zulässigkeit einer Übermittlungen von Anschriften von früheren Angestellten einer Stadt bzw. von Versorgungsempfängern, die früher im Beamtenverhältnis einer Landesbehörde tätig waren, setzt nach Art. 17 Abs. 1 BayDSG voraus, daß die Weitergabe der Anschriften zur gesetzlich zugewiesenen Aufgabenerfüllung der Bezirksfinanzdirektion bzw. der Zusatzversorgungskasse der Stadt oder der Erhebungsstelle erforderlich ist. Der Erhebungsstelle für die Volkszählung 1987 obliegt die Auswahl der Zähler. § 10 VZG sieht ausdrücklich vor, daß für die Erhebung ehrenamtliche Zähler eingesetzt werden können. Eine Pflicht zur Übernahme der Zählertätigkeit bestand nur für Personen bis zum vollendeten 65. Lebensjahr. Dies schließt allerdings eine freiwillige Übernahme des Zähleramtes durch Personen, die älter als 65 Jahre sind, nicht aus. Auf die Freiwilligkeit war allerdings deutlich hinzuweisen.

d) Gebäudevorerhebung

In die Vorbereitungsphase fiel auch die Überprüfung der Erhebungsbogen für die vorgezogene Gebäudeerhebung durch den Landesbeauftragten.

Das Volkszählungsgesetz sieht vor, daß mit der Gebäudezählung bis zu 6 Monaten vor dem Zählungsstichtag begonnen werden kann. Der Erhebungsbogen für diese vorgezogene Gebäudezählung bestand aus einem Blatt, auf dem sowohl die Anschrift des Auskunftspflichtigen und damit Hilfsmerkmale als auch die Erhebungsmerkmale standen. § 15 Abs. 2 VZG schreibt vor, daß die Hilfsmerkmale grundsätzlich unverzüglich nach Durchführung der Eingangskontrollen bei den statistischen Ämtern der Länder von den Erhebungsmerkmalen zu trennen und gesondert aufzubewahren sind. Die datenschutzrechtliche Überprüfung hat ergeben, daß das Landesamt für Statistik und Datenverarbeitung die Trennung folgendermaßen sichert: Nach Vorliegen der übrigen Erhebungsbogen der Volkszählung werden die jeweiligen Gebäudeangaben

schon in den Erhebungsstellen auf die entsprechenden Wohnungsbogen übertragen. Nach Durchführung der Eingangskontrollen durch das Landesamt für Statistik und Datenverarbeitung werden die Gebäudebogen aus der Vorerhebung zur Volkszählung 1987 vernichtet. Das Trennungsgebot des § 15 Abs. 1 VZG wird daher in Bayern durch Vernichtung des **gesamten** Bogens der Gebäudevorerhebung erfüllt.

e) Arbeitsstättenbogen

Die Überprüfung des Arbeitsstättenbogens hat ein ähnliches, in der Gestaltung des Bogens liegendes Problem aufgezeigt. Seite 1 des Arbeitsstättenbogens 1987 sieht neben den Hilfsmerkmalen auch das Erhebungsmerkmal „Gemeinde" vor. Auf meine Anfrage nach dem vorgesehenen Trennungsverfahren hat das Landesamt für Statistik und Datenverarbeitung erklärt, daß die Seite 1 **insgesamt** abgetrennt werde und getrennt von den übrigen Bogenseiten und Erhebungsmerkmalen aufbewahrt würde. Aus der Sicht des Datenschutzes ist dieses Verfahren nicht zu beanstanden.

f) ADV-Einsatz in den Erhebungsstellen

Sämtliche bekannt gewordenen Fälle von DV-Unterstützung in Erhebungsstellen wurden von mir überprüft (siehe Abschnitt technisch-organisatorischer Bereich 17.3). Ein Anlaß zu Beanstandungen ergab sich dabei nicht.

Die zur Speicherung in den automatisierten Verfahren vorgesehenen Daten und ihre Nutzung wurden überprüft und waren nicht zu beanstanden.

11.1.2. Kontrolle der Durchführung der Volkszählung

a) Kontrollbesuche in den Erhebungsstellen

Wie schon in der Vorbereitungsphase lag auch bei der Durchführung der Volkszählung das Schwergewicht der datenschutzrechtlichen Kontrollen auf der Prüfung der Einhaltung des Abschottungsgebotes. Das Ergebnis der Kontrollbesuche war insgesamt positiv. Nur vereinzelt war festzustellen, daß dem personellen Abschottungsgebot nicht Rechnung getragen war. Dies war vor allem bei kleineren Gemeinden der Fall, die auf die Beschäftigung von zusätzlichem Personal verzichtet hatten. Am häufigsten war dabei zu beanstanden, daß der geschäftsleitende Beamte gleichzeitig Leiter der Erhebungsstelle war, gleichwohl aber als geschäftsleitender Beamter tätig war. Das von mir unterrichtete Innenministerium veranlaßte umgehend eine nochmalige Überprüfung der Erhebungsstellen durch die Landratsämter. Bei der Nachprüfung konnte festgestellt werden, daß meine Forderungen inzwischen erfüllt waren.

Die Fragenbogenaktion (vgl. oben 11.1.1. b) wurde während der Durchführung der Volkszählung 1987 fortgesetzt, vor allem in Gemeinden, in denen Bürger vortrugen, die dortige Erhebungsstelle gebe Anlaß zur Besorgnis. Gravierende Mängel wurden nicht festgestellt. Die Verbesserung betrafen überwiegend den technisch-organisatorischen Bereich, wie z.B. Erlaß einer Regelung, daß für die Leerung der Briefkästen für die Volkszählung am Wochenende gesorgt ist. Soweit sich Mängel zeigten, sorgten die Erhebungsstellen für Abhilfe.

b) Bürgereingaben

Über 200 Bürger haben sich mit „Volkszählungssorgen" schriftlich an mich gewandt. Außerdem standen während der ersten sechs Wochen nach dem Stichtag 25. Mai 1987 die Telefone der Geschäftsstelle nicht mehr still – nach vorsichtiger Schätzung wurden über 1000 telefonische Anfragen beantwortet. Einige Bürger suchten persönlich die Geschäftsstelle des Landesbeauftragten auf. Bei den Bürgern, die sich an mich gewandt haben, waren nahezu alle Alters- und Bevölkerungsgruppen vertreten: Beispielsweise Mütter behinderter Kinder, die eine soziale Abstempelung ihrer Kinder befürchteten, weil für diese kein Schulabschluß in den Erhebungsbogen eingetragen werden konnte. Alte Menschen, die mehr als ein Zimmer bewohnen, hatten Angst, aufgrund ihrer wahrheitsgemäßen Angabe bei der Volkszählung könnten ihnen die übrigen Zimmer weggenommen und zwangsbewirtschaftet werden. Eine verbreitete Verunsicherung von Teilen der Bevölkerung, die durch verantwortungslose Kampagnen verängstigt war, war festzustellen.

aa) Auf die **Erhebungsstelle** bezogen sich folgende Bürgerfragen

- Darf die Erhebungsstelle ihren Briefverkehr unter dem Briefkopf der Gemeinde führen?

  Sie darf. Die Bayer. Durchführungsverordung weist die Aufgabe der örtlichen Erhebungsstellen den Gemeinden zu. Das Abschottungsgebot verlangt kein besonderes Briefpapier für die Erhebungsstellen. Dies würde auch den Datenschutz für den Bürger nicht verbessern.

- Was ist zu tun, wenn die Volkszählungsunterlagen verloren gehen?

  Das Volkszählungsgesetz bestimmt, daß die Auskunft erst dann erteilt ist, wenn die ausgefüllten Erhebungsvordrucke der Erhebungsstelle zugegangen sind. Nachweispflichtig hierfür ist der Bürger. Andernfalls hätten Volkszählungsboykotteure ein leichtes Spiel.

- Ist eine Auswertung der Erhebungsbögen durch die Gemeinden oder Erhebungsstellen vorgesehen?

  Die Volkszählung ist zwar die Grundlage für die Feststellung der amtlichen Bevölkerungszahl von Bund, Ländern und Gemeinden. Die Auswertung ist aber den statistischen Ämtern des Bundes und der Länder vorbehalten. Die amtliche Bevölkerungszahl errechnet sich aus der Zahl der Bürger, die an einem Ort ihren **Haupt**wohnsitz haben. Sie kann daher nur durch Auswertung des Inhalts der Volkszählungserhebungsbögen festgestellt werden. Solche unmittelbaren inhaltlichen Auswertungen von Angaben der Auskunftspflichtigen durch die Erhebungsstellen der Gemeinden sind vom Volkszählungsgesetz nicht zugelassen. Dies berührt nicht die Möglichkeit von Gemeinden zur Auswertung der Volkszählung gemäß § 14 Abs. 1

VZG, wenn das Landesamt für Statistik und Datenverarbeitung ihnen nach der Aufbereitung Daten (auf Blockseiten-Ebene) übermittelt.

- Darf die Meldebehörde Daten an die Erhebungsstelle übermitteln?

  Das Volkszählungsgesetz sieht ausdrücklich eine Datenübermittlung vom Meldeamt an die Erhebungsstellen zur Organisation der Volkszählung vor. Diese Datenübermittlung ist beschränkt auf die Angaben Vor- und Familiennamen, Gemeinde, Straße, Hausnummer, Haupt- oder Nebenwohnung, Geburtsjahr und -monat, Geschlecht und Staatsangehörigkeit. Diese Datenübermittlung hat mit dem im Volkszählungsgesetz 1983 vorgesehenen Melderegisterabgleich, einer Datenübermittlung von der Erhebungsstelle zum Meldeamt, nichts zu tun.

- Darf die Erhebungsstelle die Daten, die vom Meldeamt übermittelt werden, direkt in die Erhebungsbogen eintragen?

  Ein Bürger hat sich an mich gewandt, weil er vom Zähler einen Haushaltsmantelbogen ausgehändigt erhalten hat, der bereits ausgefüllt war. Die Erhebungsstelle führte dazu aus, diese Angaben seien nicht vom Zähler, sondern von der Erhebungsstelle versehentlich eingetragen worden. Dies ist nicht zulässig. Der Landesbeauftragte hat veranlaßt, daß dem Bürger unverzüglich neue Erhebungsunterlagen zugestellt wurden.

bb) Nachfolgende Fragen betrafen das Tätigwerden des 1. Bürgermeisters bei der Durchführung der Volkszählung:

- Ist die Behandlung einer Dienstaufsichtsbeschwerde durch den ersten Bürgermeister zulässig?

  Die Behandlung einer Dienstaufsichtsbeschwerde durch den ersten Bürgermeister ist nicht zu beanstanden. Diesem obliegt nach den Vorschriften der Gemeindeordnung die Dienstaufsicht über Beamte, Angestellte und Arbeiter der Gemeinde. Auch gegenüber Mitarbeitern der Erhebungsstelle ist der erste Bürgermeister der erste Dienstvorgesetzte.

- Darf der erste Bürgermeister einen Widerspruch gegen die Heranziehung zur Auskunftserteilung bei der Volkszählung behandeln?

  Das Abschottungsgebot gilt nur für die Erhebung und Verarbeitung der im Rahmen der Volkszählung erhobenen Daten. Es verlangt nicht, daß bei der Volkszählung sonst durchzuführende Verwaltungstätigkeiten ausschließlich von der Erhebungsstelle erledigt werden. Mit der Einlegung eines Widerspruchs gegen den Anforderungsbescheid bewegt sich der Widerspruchsführer selbst aus dem Schutzbereich der abgeschotteten Erhebungsstelle heraus. Er kann sich infolgedessen auch nicht mehr auf das Abschottungsgebot berufen. Rechtliche Bedenken bestehen dagegen nicht.

cc) Zum **Zählereinsatz** wurden folgende Fragen gestellt:

- Was wird der meldenden Dienststelle mitgeteilt, wenn ein benannter Zähler nicht eingesetzt wird?

  Für die Aufgabenerfüllung der öffentlichen Stellen im Rahmen der Volkszählung war es grundsätzlich ausreichend, wenn die Erhebungsstelle nur die Tatsache mitgeteilt hat, **daß** die benannten Personen nicht als Zähler eingesetzt werden. Mit dieser Information waren die öffentlichen Stellen in der Lage, gem. der Bekanntmachung der Bayer. Staatsregierung weitere Personen für den Zählereinsatz zu benennen. Eine Mitteilung darüber, aus welchem Grund es nicht zum Zählereinsatz kam, war nur dann zulässig, wenn die Mitteilung zur Erfüllung der Aufgaben der jeweiligen öffentlichen Stelle **erforderlich** war.

  Nicht erforderlich war jedenfalls die Weiterleitung von ärztlichen Gesundheitsattesten, welche Lehrer der Gemeinde vorgelegt hatten, an das Staatl. Schulamt.

- Wann liegt ein Interessenkonflikt zwischen der Tätigkeit als Zähler und der angestammten Tätigkeit vor?

  Nach § 10 Abs. 5 VZG durften Zähler nicht eingesetzt werden

  „1. in der unmittelbaren Nähe ihrer Wohnung (Nachbarschaft);

  2. wenn aufgrund ihrer beruflichen Tätigkeit oder aus anderen Gründen zu besorgen ist, daß Erkenntnisse aus der Zählertätigkeit zu Lasten der Auskunftspflichtigen genutzt werden."

  Die Erhebungsstelle mußte in manchen Fällen auch die Bewertung des Dienstherrn bzw. Arbeitgebers zur Frage der Interessenkollision mit in ihre Entscheidung einfließen lassen. Dabei hat der Erhebungsstelle in diesen Fällen regelmäßig die eigene Sachkunde gefehlt, um beurteilen zu können, ob aus der Tätigkeit bei der Volkszählung Erkenntnisse für die berufliche Tätigkeit des benannten Zählers zu Lasten der Auskunftspflichtigen nutzbar waren.

- Werden schutzwürdige Belange der Bürger verletzt, wenn der Zähler die leeren Volkszählungsunterlagen zur Aushändigung an den Auskunftspflichtigen einem Nachbarn übergibt?

  In der Übergabe der leeren Erhebungsbogen an den Nachbarn mit der Bitte, diese zu übergeben, war keine Beeinträchtigung schutzwürdiger Belange zu erkennen. Die dem Nachbarn dadurch bekanntgewordene Heftnummer war eine Ordnungsnummer, wie sie vom Volkszählungsgesetz zugelassen war. Sie ermöglichte bei der Durchführung der Zählung eine Eingangs- und Vollzähligkeitskontrolle. Die Heftnummer war weder ein Personenkennzeichen noch die Zusammenfassung bereits bekannter Informationen.

- Ist es rechtmäßig, daß die Zähler über Adressenlisten verfügen?

Dies war zulässig. Bei der Adressenliste handelte es sich um ein Organisationspapier.

Nach dem Volkszählungsgesetz waren die Zähler berechtigt, in die Erhebungsunterlagen Angaben über die Zahl der Personen im Haushalt, die Zahl der Haushalte und der Arbeitsstätten im Gebäude und in der Wohnung, die Zugehörigkeit zu ausländischen Streitkräften oder zu diplomatischen und berufskonsularischen Vertretungen oder zur Ständigen Vertretung der Deutschen Demokratischen Republik, das Leerstehen der Wohnung und die Hilfsmerkmale nach § 8 Abs. 1 Nrn. 1 und 3 VZG selbst einzutragen, soweit sie Voraussetzung für die ordnungsgemäße Durchführung der Zählertätigkeit waren. In die Adressenliste trug der Zähler alle für das Zählgeschäft wichtigen Informationen ein. Die Listen wurden wie die Haushaltsmantelbogen nach der Eingangskontrolle im Landesamt für Statistik und Datenverarbeitung von den Erhebungsmerkmalen getrennt und gesondert aufbewahrt. Sie werden spätestens zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes vernichtet.

- Darf der Verwalter eines Schwesternwohnheimes als Zähler dort eingesetzt werden?

  Das Bundesverfassungsgericht hat in seinem Urteil zum Volkszählungsgesetz 1983 zur Problematik des Interessenkonfliktes ausgeführt: „Den Bürgern treten Zähler entgegen, die Einblick in die Unterlagen erhalten, wenn der ausgefüllte Erhebungsbogen offen abgegeben wird. Deshalb müssen Maßnahmen getroffen werden, um Interessenkollisionen möglichst zu vermeiden. Dem Schutzbedürfnis wird zwar schon weitgehend durch die aufgeführten verschiedenen Möglichkeiten der Abgabe des ausgefüllten Fragebogens Rechnung getragen. Dies allein reicht jedoch bei einer Massenerhebung mit etwa 600.000 Zählern für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung nicht aus."

  Ein Interessenkonflikt konnte beim Verwalter des Wohnheimes schon dadurch gegeben sein, daß eine Beziehung vergleichbar dem Verhältnis zwischen Mieter und Vermieter besteht. Nach den Ausführungen der Erhebungsstelle wurde es von dort als hilfreich angesehen, wenn ein Zähler eingesetzt war, der die besonderen Verhältnisse bei seiner Zählertätigkeit berücksichtigen konnte, die besonderen Gepflogenheiten kannte sowie für Rückfragen bei auftretenden Fragen zu den Wohnungen zur Verfügung stand. Gerade in der Kenntnis der besonderen Verhältnisse und Gepflogenheiten sehe ich jedoch ein Indiz für einen Interessenkonflikt. Ich habe diesen Zählereinsatz beanstandet.

- Ist es zulässig, daß der Hausmeister eines Studentenwohnheimes dort als Zähler eingesetzt wird?

  Wie im Fall des Verwalters ist auch dieser Zählereinsatz unzulässig. Aufgrund der Tätigkeit als Hausmeister in eben diesem Studentenwohnheim ist ein Interessenkonflikt schon dann gegeben, wenn z.B. ein Student einen anderen Studenten bei sich wohnen läßt und damit gegen die Hausordnung verstößt. Unrichtige Angaben sind dann nicht auszuschließen.

- Darf der Mitarbeiter eines Arbeitsamtes, der bei der Entgegennahme von Anträgen von Arbeitslosen mitwirkt, als Zähler eingesetzt sein?

  Auch dieser Zählereinsatz war unzulässig. Ein Interessenkonflikt konnte bei dem Mitarbeiter des Arbeitsamtes beispielsweise dann auftreten, wenn ein Auskunftspflichtiger, der im Rahmen der Volkszählung Angaben zur Arbeitsstätte macht, später einen Antrag auf Arbeitslosengeld stellte.

- Dürfen Verwaltungsbeamte, Angestellte und Arbeiter aus dem Polizeibereich als Zähler eingesetzt werden?

  Als Zähler schieden die im Vollzugsdienst tätigen Dienstkräfte der Polizei aus. Dies war auch durch entsprechende Anweisungen sichergestellt. Bei den übrigen Personen war im Einzelfall zu prüfen, ob die Voraussetzungen eines Interessenkonfliktes vorliegen. Allein die Tatsache, daß jemand in einem Polizeipräsidium tätig ist, stand seinem Einsatz als Zähler noch nicht grundsätzlich entgegen. So bestanden keine Bedenken, wenn Personen, die im Bereich der Materialverwaltung oder der Kfz-Wartung tätig sind, als Zähler eingesetzt wurden.

- Wann liegt ein Zählereinsatz in der Nachbarschaft vor?

  Der Gesetzgeber hat den Bereich der Nachbarschaft nicht festgelegt.

  Nach den Vorgaben des Landesamtes für Statistik und Datenverarbeitung als oberster Erhebungsstelle durfte ein Zähler keinesfalls in der zu seiner Wohneinheit gehörende Blockseite bzw. in diesem Straßenabschnitt eingesetzt werden. Eine konkrete Definition des Begriffs „Nachbarschaft", etwa durch Festlegung einer Luftlinien-Entfernung war wegen der zu unterschiedlichen örtlichen Verhältnisse nicht möglich.

  In allen Gemeinden, von denen dem Landesbeauftragen rechtzeitig bekannt wurde, daß Zähler in der Nachbarschaft zum Einsatz vorgesehen waren oder tatsächlich eingesetzt waren, konnte der Datenschutzbeauftragte einen Austausch veranlassen.

- Dürfen den Erhebungsstellen und Zählern die Nachnamen von in Adoptivpflege lebenden Kindern mitgeteilt werden?

  Bei Adoptionspflegschaften (Pflegschaften, in denen das Adoptionsverfahren noch nicht abgeschlossen ist und die Kinder noch nicht den Familiennamen der Adoptiveltern tragen) besteht zwar ab dem Zeitpunkt der Einwilligung der

leiblichen Eltern gem. den Vorschriften des bürgerlichen Gesetzbuches eine Auskunftssperre nach dem Melderecht. Diese gilt jedoch nicht gegenüber Behörden. Daher war es zulässig, wenn die Meldebehörden den Erhebungsstellen die Namen und die sonst in § 11 Abs. 1 VZG genannten Daten der in Adoptivpflegschaft lebenden Kinder mitgeteilt haben und diese sie an die Zähler weitergegeben haben. Dies führte nun in einzelnen Fällen, in denen der Zähler die Erhebungsunterlagen einem Nachbarn zur Aushändigung an die Adoptionseltern gegeben hat, dazu, daß dem Nachbarn die Tatsache der Adoptionspflegschaft bekannt wurde.

Auch wenn das geschilderte Verfahren zulässig war, ist es doch aus der Sicht des Datenschutzes bedauerlich, daß die Problematik offenbar nicht rechtzeitig erkannt wurde. Möglicherweise hätte man eine für die Betroffenen befriedigendere Lösung finden können.

dd) Bürgerfragen zur Anonymität der Volkszählung

Die Volkszählung ist keine anonyme Datenerhebung. Name und Anschrift sind für die Volkszählung erforderlich. Diese Daten werden von den örtlichen Erhebungsstellen, z.B. zur Adressierung von Schreiben, für Rückfragen, zur Kontrolle, ob die ausgegebenen Erhebungsvordrucke zurückgesandt wurden, und auch für Erinnerungs- und Mahnschreiben verwendet. Der jeweilige Bearbeitungsstand wird festgehalten. So wurde beispielsweise vermerkt, daß die Rücksendung der Erhebungsvordrucke per Post angekündigt wurde. Unmittelbar nach Abschluß der Volkszählungsarbeiten in den örtlichen Erhebungsstellen werden die Erhebungsvordrucke und die den Erhebungsstellen zur Organisation der Zählung übermittelten Daten der Einwohner an das Landesamt für Statistik und Datenverarbeitung übersandt. Alle übrigen bei der Erhebungsstelle vorhandenen personenbezogenen Daten der Befragten werden vernichtet. Ausgenommen sind nur die Daten der Personen, die ihrer Auskunftspflicht nicht nachgekommen sind. Diese Daten können zur Durchführung von Ordnungswidrigkeiten- oder Verwaltungsvollstreckungsverfahren an die dafür zuständigen Stellen weitergeleitet werden.

Bei der weiteren statistischen Bearbeitung im Landesamt müssen die Namen und Vornamen auf den Erhebungsvordrucken zum frühest möglichen Zeitpunkt von den Erhebungsmerkmalen getrennt werden. Sie werden nicht auf elektronische Datenträger übernommen.

Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil 1983 ausgeführt, daß es zur Sicherung des Rechts auf informationelle Selbstbestimmung besonderer Vorkehrungen bedürfe für Durchführung und Organisation der Datenerhebung und -verarbeitung, da die Informationen während der Phase der Erhebung und zum Teil auch während der Phase der Speicherung noch individualisierbar sind. Das Bundesverfassungsgericht geht selbst von einer nicht anonymen Speicherung innerhalb der Statistischen Ämter aus. Das Gebot der (faktischen) Anonymisierung hat nur Bedeutung im Außenverhältnis. Dies wird auch deutlich herausgestellt. Zunächst fordert das Gericht „Vorkehrungen für Durchführung und Organisation der Datenerhebung und -verarbeitung" (BVerfGE 65, Seite 49), dann erst führt es aus: „Von besonderer Bedeutung für Statistische Erhebungen sind wirksame **Abschottungsregelungen nach außen**". Der Schutzzweck der faktischen Anonymisierung besteht darin, einem Datenmißbrauch außerhalb des abgeschotteten Statistikbereiches zu begegnen.

In der jüngsten Rechtsprechung des Bundesverfassungsgerichts (Beschluß vom 24.9.1987 – 1 BvR 970/87 -) ist dazu folgendes ausgeführt: „Von Verfassung wegen gefordert ist lediglich eine faktische Anonymität der Daten. Diese kann – in Anlehnung an § 16 Abs. 6 Bundesstatistikgesetz – allenfalls dann als gegeben angesehen werden, wenn Datenempfänger oder Dritte eine Angabe nur mit einem – im Verhältnis zum Wert der zu erlangenden Information nicht zu erwartenden – unverhältnismäßig großen Aufwand an Zeit, Kosten, Arbeitskraft und sonstigen Ressourcen (etwa Risiko einer Bestrafung) einer Person zuordnen können. ... Für die Statistischen Landesämter bleiben die Daten allerdings durchgängig personenbezogen, weil personenbeziehbar."

– Die Anonymitätsfrage wurde in Eingaben auch im Zusammenhang mit den Fragen 12 bis 14 des Personenbogens gestellt, wenn der Auskunftspflichtige ein Selbständiger war, der auf seinem Wohngrundstück auch seiner Arbeit nachging.

  In Frage 12 des Personenbogens wurde nach Name und Anschrift der Arbeitsstätte oder Schule/Hochschule gefragt. Frage 13 verlangte Angaben zum Verkehrsmittel, das auf dem Weg dorthin benutzt wird. In Frage 14 schließlich ging es darum, wieviel Zeit für den Hinweg üblicherweise benötigt wird. Als eine Antwortmöglichkeit war angeboten „entfällt, da auf gleichem Grundstück". Ein Selbständiger, der auf seinem Wohngrundstück auch arbeitete, gab danach in Frage 12 den eigenen Namen und die eigene Anschrift an.

  Eine Vielzahl von Selbständigen fühlte sich dadurch wegen mangelnder Anonymität belastet. Das Volkszählungsgesetz deckte diese Datenerhebung auch dann, wenn der Auskunftspflichtige ein Selbständiger war.

  Davon abgesehen hat mir das Landesamt für Statistik und Datenverarbeitung versichert, daß bei Selbständigen in Frage 12 auf den Namen der Arbeitsstätte verzichtet werden konnte. Die Daten Name, Straße, Hausnummer, Postleitzahl und Gemeinde der Arbeitsstätte würden nicht maschinell übernommen. Die Personenbogen würden unsortiert bearbeitet und aufbewahrt; insbesondere seien sie nicht danach sortiert, ob ein Selbständiger die Frage 12 beantwortet habe oder ein Arbeitnehmer. Eine Sonderbehandlung und -bearbeitung der Personenbogen der Selbständigen würde umgekehrt die Reidentifizierungsmög-

lichkeit sogar erhöhen und den Datenschutz mindern.

ee) Teilnahme des Datenschutzbeauftragten an öffentlichen Diskussionen

Auf Bitten zahlreicher Initiatoren von Informationsveranstaltungen über die Volkszählung hat der Landesbeauftragte für den Datenschutz in vielen Fällen an solchen Veranstaltungen teilgenommen. Dabei hat mein Vorgänger jedoch Wert darauf gelegt, daß in der Regel auch Vertreter der zuständigen Statistikstellen teilnehmen.

11.1.3. Tätigkeit des Datenschutzbeauftragten in der Abgabephase

Was passiert in den Erhebungsstellen, wenn die Volkszählungsunterlagen über das Landratsamt an das Landesamt für Statisik und Datenverarbeitung abgegeben sind?

Nach der Abgabe der Erhebungsbogen beim Landesamt überwacht der Landesbeauftragte die weiteren Abläufe. Unproblematisch sind die Fälle, in denen eine Erhebungsstelle sämtliche Erhebungsunterlagen erhalten hat und weiterleiten konnte. Fragen tauchen auf, wenn einzelne Bürger ihre Unterlagen noch nicht abgegeben haben und gegen sie Zwangsgeld-Beitreibungsverfahren eingeleitet sind, die Masse der Unterlagen aber abgegeben ist. Für die Abwicklung dieser ausstehenden Erhebungsfälle hat das Staatsministerium des Innern den Gemeinden zwei Verfahrenswege angeboten, die mit mir abgestimmt wurden:

a) Eingehende Volkszählungspost wird einem für die Tätigkeit in der Erhebungsstelle geeigneten Bediensteten zugeleitet. Er verwahrt die Post ungeöffnet und abgeschottet. Sobald ausreichend Post eingegangen ist, teilt der Bedienstete dem ersten Bürgermeister mit, daß die Erhebungsstelle wieder zu besetzen sei. Dies wird angeordnet. Nach Bearbeitung des Posteingangs ist die Erhebungsstelle wieder unbesetzt.

b) Die Gemeinde leitet eingehende Volkszählungspost im verschlossenen Umschlag über das Landratsamt an das Landesamt für Statistik und Datenverarbeitung weiter, wo sie erstmals geöffnet wird. Sofern für die Gemeinde der Absender erkennbar ist, setzt sie gleichzeitig ein gegen den Absender eingeleitetes Zwangsgeld-Beitreibungsverfahren aus.

Das Landesamt für Statistik und Datenverarbeitung überprüft die eingehende Post unverzüglich und teilt der Gemeinde mit, in welchen Fällen die Auskunftspflicht erfüllt ist. Die Gemeinde veranlaßt dann die (endgültige) Einstellung des Beitreibungsverfahrens.

Stellt das Landesamt fest, daß die Auskunftspflicht – ganz oder teilweise – nicht erfüllt ist, so teilt es dies **ohne zusätzliche Einzelheiten** der Gemeinde mit.

11.1.4. Zur Wiederholungsbefragung

Das Landesamt für Statistik und Datenverarbeitung unterrichtete mich über die Durchführung der Wiederholungsbefragung und den Inhalt der hierzu verwendeten Erhebungsbogen. Die datenschutzrechtliche Überprüfung ergab keinen Grund zur Beanstandung.

Die Wiederholungsbefragung betraf 63 Gemeinden und etwa 11.000 Personen. Zweck dieser Wiederholungsbefragung ist es, die Vollzähligkeit und Zuverlässigkeit der Zählungsergebnisse der Haupterhebung im Sommmer zu überprüfen. Es werden nochmals Daten zum Stichtag 25. Mai 1987 festgestellt. Der Datenumfang ist allerdings beschränkt auf 6 Fragen, nämlich Angaben zu Geburt, Geschlecht, Familienstand, Staatsangehörigkeit, Wohnung und Erwerbstätigkeit.

Zählerprobleme sind bei dieser Wiederholungsbefragung von vornherein ausgeschlossen, da nur Bedienstete des Landesamtes für Statistik und Datenverarbeitung für das Zählgeschäft eingesetzt sind.

11.1.5. Kontrolltätigkeit beim Landesamt für Statistik und Datenverarbeitung

Zu Beginn des Jahres 1988 werde ich beim Landesamt für Statistik und Datenverarbeitung die Einhaltung der Datensicherungsmaßnahmen und die Einhaltung der rechtlichen Vorgaben für die Weiterbearbeitung der Volkszählungsdaten überprüfen.

11.1.6. Resümee zum Datenschutz bei der Volkszählung

Der Landesbeauftragte mußte bei seiner umfangreichen Kontrolltätigkeit keine Feststellungen treffen, die die Volkszählung in Frage gestellt hätten. Die Forderungen des Datenschutzbeauftragten wurden akzeptiert und im wesentlichen auch eingehalten. Ich danke allen Gemeinden und staatlichen Stellen für die Unterstützung, die ich im Rahmen meiner Kontrolltätigkeit erfahren habe.

11.2. Mikrozensus

Bei jeder Mikrozensuserhebung wenden sich Bürger an mich. Sie wollen sich vergewissern, ob die umfangreiche Erhebung zulässig ist. Das Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) vom 10.6.1985 entspricht bereits den Anforderungen, die das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 an ein Statistikgesetz gestellt hat. Dort ist genau festgelegt, welche Merkmale Erhebungsmerkmale und welche Hilfsmerkmale sind. Auch das Gebot zur Trennung und Löschung ist beachtet.

11.3. Erhebungen zur amtlichen Schulstatistik

Anläßlich der Eingabe einer privaten Berufsfachschule habe ich den Datenumfang der amtlichen Schulstatistik überprüft. Von der Berufsfachschule war gerügt worden, daß Angaben zur Staatsangehörigkeit der Schüler sowie zur „schulischen Vorbildung" zu machen sind. Diese Daten würden für eigene Zwecke dieser Schule von den Schülern nicht erhoben, da sie für die Ausbildung keine Rolle spielten.

Die Überprüfung ergab keinen Anlaß zur Beanstandung. Auf der Grundlage der Genehmigung des statistischen Genehmigungsausschusses vom 18.7.1972 werden die jährlichen Befragungen der allgemeinbildenden sowie der beruflichen Schulen als koordinierte Landesstatistik durchgeführt. Diese Genehmigung gilt als Rechtsvorschrift im Sinne des Bayerischen Datenschutzgesetzes (vgl. Art. 23 BayDSG). Danach sind die Schulen verpflichtet, die in der Genehmigung aufgeführten und in den Erhebungsunterlagen vorgesehenen Daten an die Aufsichtsbehörde zu liefern. Hierzu müssen sie die entsprechenden Merkmale von den Schülern erheben. Nach den Vorschriften des Bayerischen Erziehungs- und Unterrichtsgesetzes ist die Erhebung und

Verarbeitung von Daten zur Erfüllung der den Schulen durch Rechtsvorschrift jeweils zugewiesenen Aufgaben erforderlich und zulässig. Die Daten werden für Zwecke der Bildungsplanung, zur Verfolgung der Schülerströme und für die Prognose der künftigen Schülerzahlen im Bereich der Berufsfachschulen benötigt. Zu Planungen des Staatsministeriums für Unterricht und Kultus zur Gestaltung der Schulstatistik siehe Nr. 12.2.3.

12. Schule und Hochschule

12.1. Hochschulwesen

12.1.1. Datenschutzrechtliche Prüfung der Ludwig-Maximilians-Universität München

Schwerpunkt meiner Kontrolltätigkeit im Hochschulbereich war im Berichtszeitraum eine datenschutzrechtliche Prüfung bei der Ludwig-Maximilians-Universität München. Meine besondere Aufmerksamkeit richtete sich dabei auf die automatisierte Studentendatei der Universität. Daneben habe ich eine Reihe weiterer automatisierter Dateien geprüft. Hierzu gehörten u. a. die Zulassungsdatei, die Studentenwerk-Beitragsdatei, die Studienförderungsdatei, die Datei für Auswahlgespräche (Medizin), die Datei für die Anmeldung zu den medizinischen Pflichtveranstaltungen, die Wahldatei und die Personaldatei.

Die einzelnen Datenfelder der vorbezeichneten Dateien habe ich unter dem Gesichtspunkt der Erforderlichkeit einer Daten**speicherung** überprüft. Durchgreifende Bedenken waren nicht zu erheben. Ich habe freilich festgestellt, daß z. B. die Datenfelder „Art der Beurlaubung" und „Grund des Ausscheidens" der automatisierten Personaldatei mit Schlüsselkennzeichen belegt werden können, die eine sehr detaillierte Erfassung von Informationen zulassen. So kann z. B. gespeichert werden, ob der Betroffene Erholungsurlaub genommen hat oder erkrankt ist. Viele der hier festgestellten Varianten werden nach Auskunft der Universitätsverwaltung in der Praxis nicht benötigt. Ich habe deshalb angeregt, die maßgebenden Schlüsselverzeichisse unter dem Gesichtspunkt der Erforderlichkeit und auch zur Vermeidung unnötiger Bürokratie zu überarbeiten.

Weiter war Gegenstand der Prüfung die Frage der Daten**löschung** (Aussonderung) und der **Archivierung**. Auch hier konnten aus datenschutzrechtlicher Sicht Mängel von Gewicht nicht festgestellt werden. Ich habe der Universität allerdings empfohlen, die weitere Vorhaltung und Nutzung archivierter Studentendaten durch universitätsinterne Aufbewahrungsbestimmungen rechtlich genauer zu regeln. Dabei wäre zu berücksichtigen, daß jedenfalls statusrechtliche Unterlagen (z. B. über bestandene Prüfungen, Promotionen) zumindest bis zum Tod des Betroffenen aufbewahrt werden müssen. Andere Daten (z. B. Semesteradresse), die die Universität nicht mehr benötigt, können dagegen gelöscht werden, um Kapazitätsproblemen zu begegnen, sofern kein Grund zu der Annahme besteht, daß hierdurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

In einer anderen Datei, deren Daten nicht archiviert werden, erfolgt die Datenlöschung durch Überschreibung des Dateiinhalts. Ich habe angeregt, diese Praxis zu überprüfen. Das Risiko einer fehlerhaften Erfassung der neuen Daten sollte vermieden werden, das hier immer dann auftritt, wenn ein alter Datensatz nicht in jedem Feld lückenlos überschrieben wird.

Die von mir im Rahmen der Prüfung weiter erholten Stichproben aus den einzelnen Dateien ergaben keinen Anlaß zur Beanstandung.

Einer Stellungnahme der Universität zu meinem Prüfbericht sehe ich noch entgegen. Dennoch kann ich bereits jetzt feststellen, daß die Ludwig-Maximilians-Universität München den datenschutzrechtlichen Belangen erhebliches Gewicht beimißt. Die Persönlichkeitsrechte der Studenten und Bediensteten werden bei der automatisierten Datenverarbeitung gewahrt.

12.1.2. Automation in der Hochschulverwaltung (DIAPERS)

Erneut beschäftigt hat mich im Berichtszeitraum das dialogorientierte Stellen- und Personalverwaltungssystem DIAPERS, das derzeit an der Universität Erlangen-Nürnberg im Testeinsatz erprobt wird. Gegenstand meiner Bemühungen ist hier vor allem die Frage der Erforderlichkeit der vorgesehenen Datenspeicherung. Derzeit sind im wesentlichen noch zwei Problemkreise offen:

Zum einen halte ich in Übereinstimmung mit dem Staatsministerium der Finanzen die detaillierte Erfassung der rechtlichen Stellung von Kindern Betroffener (z. B. Offenlegung einer Adoption) für Zwecke der Bezügeabrechnung nicht für erforderlich. Gleiches gilt für die Erfassung der Teilnahme von Bediensteten an Forschungsprojekten zum Zwecke eines Finanzierungsnachweises im Rahmen der Drittmittelförderung. Je nach Brisanz des Forschungsprojekts wird zumindest im Einzelfall ein erhebliches Interesse des Betroffenen an einer möglichst weitgehenden Geheimhaltung seiner Beteiligung anzuerkennen sein. Ich habe Zweifel, ob angesichts dessen die vorgesehene Datenspeicherung hier noch durch die beamtenrechtlichen Personalverwaltungskompetenzen gedeckt wird, die üblicherweise keine derart genaue Erfassung der Tätigkeit eines Bediensteten erforderlich machen.

Im übrigen bedarf die Dienstanweisung für den Einsatz von DIAPERS an der Universität Erlangen-Nürnberg aus meiner Sicht noch ergänzender Hinweise zu technisch-organisatorischen Fragen.

Zur weiteren Abklärung der aufgezeigten Probleme werde ich mich demnächst erneut mit dem Staatsministerium für Wissenschaft und Kunst in Verbindung setzen.

12.1.3. Änderung des Bayerischen Hochschulgesetzes

Das Staatsministerium für Wissenschaft und Kunst hat mir vor kurzem einen Gesetzentwurf zur Änderung des Bayerischen Hochschulgesetzes (Stand: Oktober 1987) zugeleitet. Anlaß für das recht umfassend angelegte Gesetzgebungsvorhaben ist eine Änderung des Hochschulrahmenrechts des Bundes. Die Länder sind verpflichtet, ihr Hochschulrecht entsprechend anzupassen.

In meiner Stellungnahme zu dem Gesetzentwurf habe ich mich dafür ausgesprochen, in das Bayerische Hochschulgesetz – entsprechend einem Vorentwurf des Staatsministeriums für Wissenschaft und Kunst – eine Regelung jedenfalls zur Erhebung personenbezogener Daten bei den Studenten aufzunehmen, um Auseinandersetzungen über die Zulässigkeit der zu Verwaltungszwecken erforderlichen Datenerhebung möglichst von vornherein zu vermeiden. Das

Bayerische Datenschutzgesetz enthält bekanntlich bisher keine allgemeine Regelung zur Zulässigkeit einer Erhebung personenbezogener Daten.

12.1.4. Einzelfälle

Aus den Eingaben, die mich zu datenschutzrechtlichen Fragen aus dem Hochschulbereich erreicht haben, möchte ich folgende Fälle herausgreifen:

- Ein Student einer bayerischen Universität erhielt bei der Ausleihe eines Buches aus der Universitätsbibliothek einen Fristreifen, auf dem das Rückgabedatum vermerkt war. Auf der Rückseite des Streifens waren reidentifizierbar eine Vielzahl personenbezogener Daten nicht näher ermittelter Betroffener (Geburts- und Adreßdaten) aufgedruckt.

  Meine Nachforschungen ergaben, daß es sich bei den Fristreifen um veraltete Namenslisten von Studenten aus dem Rechenzentrum der Universität handelte, die zur Behebung eines „akuten Materialmangels" in zerteilter Form zweckentfremdet worden waren. Datenschutzrechtliche Bedenken der Universitätsbibliothek hatten allerdings schon vor Beginn meiner Ermittlungen dazu geführt, daß diese Praxis wieder beendet worden war. Der zuständige Abteilungsleiter hat den Vorfall dennoch zum Anlaß genommen, alle betroffenen Bediensteten nochmals darauf hinzuweisen, daß Belege mit geschützten Daten auch nicht in vermeintlich unbedenklichen Teilen weiterverwendet werden dürfen, sondern zu vernichten sind. Ich teile diese Auffassung und gehe davon aus, daß sich Vorfälle der geschilderten Art künftig nicht mehr wiederholen werden.

12.2. Schulwesen

12.2.1. Automatisierte Schülerdateien

Bayern nimmt mit seinem schulischen Unterrichtsangebot in Informatik und mit der inzwischen erreichten Rechnerausstattung der Schulen einen Spitzenplatz in der Bundesrepublik Deutschland ein. Computer werden aber nicht nur im Unterricht, sondern auch zur Unterstützung der an den Schulen anfallenden Verwaltungsarbeiten eingesetzt. Dies hat zur Einrichtung **automatisierter Schülerdateien** an vielen bayerischen Schulen geführt. Eine automatisierte Schülerdatei enthält in der Regel Name, Vorname und andere persönliche Daten der betroffenen Schüler, Adreßdaten, Daten der Erziehungsberechtigten, aktuelle schulische Daten, Daten zur schulischen Vorbildung und Berufsausbildung (Berufsschulen) sowie Fach- und Leistungsdaten. Die Daten können zur Erstellung von Zeugnissen und anderen schulischen Zwecken genutzt werden.

Freilich birgt die kombinierte Nutzung von Computern zu Unterrichts- und Verwaltungszwecken auch die Gefahr eines mißbräuchlichen Zugriffs Unbefugter auf die im Verwaltungssystem erfaßten Daten in sich. Dem Datenschutz kommt deshalb gerade hier besondere Bedeutung zu. Das Staatsministerium für Unterricht und Kultus hat dies auch von Anfang an erkannt. Schon im Jahre 1979 sind „Erläuternde Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" ergangen, die den Schulen das Verständnis datenschutzrechtlicher Bestimmungen erleichtern sollten. Inzwischen hat mir das Staatsministerium mitgeteilt, daß beabsichtigt ist, die „Erläuternden Hinweise" neu zu fassen. Hierbei soll u. a. auch das bereichsspezifische Datenschutzrecht (insbesondere Art. 62 BayEUG) aufgenommen werden. Außerdem sollen neben dem Datensatz der bayerischen Schulverwaltungsprogramme u. a. auch Beispiele für die regelmäßige Übermittlung personenbezogener Daten an außerschulische Stellen (Gastschülerlisten, Jahresberichte, Erstellung von Schülerlisten für das Gesundheitsamt) aufgezeigt werden.

Ich begrüße diese Initiative des Staatsministeriums für Unterricht und Kultus. Im einzelnen habe ich in meiner Stellungnahme zu dem vorgelegten Entwurf noch einige kleinere Änderungen vorgeschlagen, die ich an dieser Stelle allerdings nicht näher erläutern möchte. Herausgreifen möchte ich lediglich das Problem der **Gastschülerlisten,** das mich auch in anderem Zusammenhang schon mehrfach beschäftigt hat.

Hierzu ist folgendes zu bemerken:

Die Schulen übermitteln in der Regel personenbezogene Daten von Schülern an den Träger des Sachaufwandes, die dieser zur Erfüllung seiner Aufgaben nach dem Bayerischen Schulfinanzierungsgesetz benötigt. Hierzu gehört auch die Erhebung eines Beitrages für Gastschüler. Das sind z. B. bei Volksschulen Schüler, die ihren gewöhnlichen Aufenthalt nicht im Sprengel der besuchten Schule haben. Kostenschuldner ist in diesem Falle die Aufenthaltsgemeinde. Ausweislich der bei mir ständig in großer Zahl eingehenden Meldungen von Schulverwaltungsprogrammen zum Datenschutzregister verfährt die Praxis derzeit bei regelmäßigen Datenübermittlungen aus automatisierten Schülerdateien an außerschulische Stellen in hohem Maße uneinheitlich. So werden etwa an den Aufwandsträger in einigen Fällen nur Name, Geburtsdatum und Adresse der betroffenen Schüler übermittelt. Teilweise wird eine umfangreichere „Gastschülerliste" übermittelt. In einem Fall sollte aber auch schon einmal der gesamte Datensatz der betroffenen Schüler mit Ausnahme der Leistungsdaten weitergegeben werden. Dies habe ich mangels Erforderlichkeit für unzulässig erklärt. Insgesamt scheint mir hier eine einheitliche Handhabung wünschenswert.

Auch im übrigen wirft die **regelmäßige Übermittlung** personenbezogener Daten an außerschulische Stellen in der Praxis noch vielfach Probleme auf. So werden teilweise im Jahresbericht der Schulen (oder in sonstiger Weise) Daten von Schülern über den nach Art. 62 Abs. 3 BayEUG zulässigen Umfang hinaus offenbart. Dem Gesetz zufolge dürfen im Jahresbericht Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schüler sowie Angaben über besondere schulische Tätigkeiten und Funktionen einzelner Schüler enthalten sein. In der Praxis enthalten die Jahresberichte den Datenschutzregistermeldungen zufolge immer wieder auch andere Daten, insbesondere Adreßdaten. Dies ist nicht zulässig.

Eine Auswertung der bei mir eingegangenen **Meldungen zum Datenschutzregister** läßt im übrigen hier noch folgende Hinweise angezeigt erscheinen: Eine meldepflichtige Datenübermittlung liegt nicht vor, wenn Bediensteten der Schule (insbesondere Lehrern) Daten über Schüler allein zu schulischen Zwecken zur Verfügung gestellt werden. Die Daten werden hier lediglich ihrer Bestimmung entsprechend innerhalb der speichernden Stelle genutzt. Ebenfalls keine meldepflichtige Datenübermittlung liegt in der Weitergabe

statistischer Angaben an die Aufsichtsbehörden oder an andere Stellen. Es fehlt hier ein Personenbezug. Beide Vorgänge werden mir häufig als „regelmäßige Datenübermittlungen" aus einem automatisierten Schulverwaltungsprogramm angezeigt. Meldungen dieser Art sind nicht erforderlich.

Das Staatsministerium für Unterricht und Kultus hat kürzlich in einem mir zur Kenntnis gebrachten Schreiben an eine Volksschule deutlich gemacht, daß künftig von den Schulen selbst entwickelte oder käuflich erworbene **Schulverwaltungsprogramme** nur mehr in begründeten Ausnahmefällen freigegeben werden. Den Schulen wird empfohlen, die bayerischen Schulverwaltungsprogramme zu nutzen, die jeder Schule kostenlos zur Verfügung gestellt werden. Ich begrüße dies als einen weiteren Schritt hin zu einer größeren Vereinheitlichung der Datenverarbeitung an den Schulen, die wie gezeigt, nicht nur aus fachlicher, sondern auch aus datenschutzrechtlicher Sicht dringend anzustreben ist.

12.2.2. Automatisierte Lehrerdateien

In meinem 8. Tätigkeitsbericht habe ich bereits ausführlich über die Automatisierung der Personalverwaltung im Geschäftsbereich des Staatsministeriums für Unterricht und Kultus berichtet. Im Berichtszeitraum wurden die Bemühungen zur Einrichtung automatisierter Systeme weiter fortgesetzt. Neben die Ebenen Staatsministerium (Lehrerdatei), Regierungen und Schulämter ist als weitere (unterste) Ebene die einzelne Schule getreten. Die vermehrte Ausstattung der Schulen mit Rechnern hat dazu geführt, daß neben Schülerdaten (vgl. oben) auch Personaldaten der Lehrer im Rahmen der den Schulen insoweit erwachsenen Aufgaben automatisiert verarbeitet werden. Nach einem vom Staatsministerium für Unterricht und Kultus vorgesehenen Datenkatalog dürfen neben persönlichen Daten der Lehrkräfte auch Daten über Zugang, Abgang und Verfügbarkeit, Daten zum Lehramt und Beschäftigungsverhältnis, zu den Unterrichtsstunden sowie zu den unterrichteten Klassen und Fächern gespeichert werden.

Ich begrüße die geplante Festlegung eines solchen Datenkataloges durch das Staatsministerium für Unterricht und Kultus, weil dadurch falschen Vorstellungen über den Inhalt von Personalverwaltungsdateien vor Ort von vornherein entgegengewirkt wird. Die Notwendigkeit solcher Festlegungen zeigt ein Einzelfall, in dem ich aufgrund einer Eingabe festgestellt habe, daß in einer (allerdings manuell geführten) Lehrerdatei einer Grundschule u. a. Familienstand, Kinderzahl und Bankverbindung der Lehrer erfaßt waren. Für die Erfüllung schulischer Aufgaben war dies im konkreten Fall nicht erforderlich. Die Regierung von Schwaben wurde vom Bayerischen Staatsministerium für Unterricht und Kultus beauftragt, der Schule mitzuteilen, daß künftig von einer Erhebung dieser Daten abzusehen ist.

Das Hauptproblem der Personalverwaltungssysteme im Geschäftsbereich des Staatsministeriums für Unterricht und Kultus liegt aus datenschutzrechtlicher Sicht nach wie vor in der Entwicklung eines abgestimmten Gesamtkonzepts unter Berücksichtigung der Personalverwaltungskompetenzen auf den verschiedenen Ebenen. Ich habe dieses Problem bereits in meinem 8. Tätigkeitsbericht im einzelnen dargestellt und möchte deshalb an dieser Stelle auf Wiederholungen verzichten. Das Staatsministerium für Unterricht und Kultus hat, wie berichtet, zur Erarbeitung eines einheitlichen EDV-Konzepts für die Personalverwaltung eine Arbeitsgruppe gebildet, die ihre Tätigkeit bisher noch nicht abgeschlossen hat.

12.2.3. Schulstatistik

Das Staatsministerium für Unterricht und Kultus plant eine verbesserte Koordination in der Schulstatistik. Kernpunkt der Überlegungen ist, statistische Daten künftig in größerem Umfang als bisher anonymisiert, aber auf den Einzelfall bezogen und nicht mehr schwerpunktmäßig in aggregierter Form (Summendaten) zu erheben. Hierdurch soll erreicht werden, daß die für die verschiedenen Zwecke benötigten statistischen Daten nur jeweils einmal erhoben werden müssen; aus den gesammelten „Individualdaten" können dann ohne weitere Datenerhebungen alle erforderlichen Auswertungen gewonnen werden. Ausgangsmaterial für die Statistik sollen im wesentlichen die zu Verwaltungs- oder Aufsichtszwecken erhobenen Schüler- und Lehrerdaten sein.

Aus datenschutzrechtlicher Sicht stellt sich als Hauptproblem dieses Verfahrens die hinreichende Anonymisierung der zu erhebenden „Individualdaten" dar. Auch ohne Nennung eines Namens können die über den einzelnen Betroffenen gewonnenen Informationen je nach Lage des Einzelfalles mehr oder weniger eindeutig auf seine Person hinweisen, so daß ein Personenbezug wieder hergestellt wäre. Es sind deshalb Vorkehrungen zu treffen, die eine Reidentifizierung des Betroffenen soweit wie möglich erschweren. Die Entscheidung des Staatsministeriums für Unterricht und Kultus über das weitere Vorgehen in dieser Angelegenheit bleibt zunächst abzuwarten. Mir wurde weitere Beteiligung zugesagt, sobald die Planungen ein konkreteres Stadium erreicht haben. (Siehe auch 11.3)

12.2.4. Einzelfälle

Aus den Eingaben und Anfragen, die mich zu Fragen des Datenschutzes im Schulwesen erreicht haben, möchte ich folgende Fälle herausgreifen:

- Daten von Schulabgängern an Krankenkassen

  Auch in den an mich herangetragenen Einzelfällen spielte häufig die Frage der Zulässigkeit einer Übermittlung von Schülerdaten an außerschulische Stellen eine Rolle. So wurde ich beispielsweise mit dem Schreiben einer Krankenkasse konfrontiert, die zu Zwecken der Mitgliederwerbung von einem Münchner Gymnasium Daten von Schulabgängern erhalten wollte. In Übereinstimmung mit dem Staatsministerium für Unterricht und Kultus habe ich die Auffassung vertreten, daß nach Art. 62 Abs. 2 BayEUG eine Übermittlung von Schülerdaten hier nicht zulässig ist, da ein Herausgabeanspruch der Krankenkasse rechtlich nicht zu begründen ist.

- Adressen von Entlaßschülern für den Bürgermeister

  Auf einen weiteren Fall der Herausgabe von Schülerdaten wurde ich im Berichtszeitraum gleich mehrfach hingewiesen. Der Vorsitzende eines Schulverbandes hatte den Leiter einer Hauptschule um Bekanntgabe der Adressen aller Entlaßschüler gebeten, um diesen ein Buchgeschenk übermitteln zu können. Nach Erhalt der Adressen wandte er sich an die entlassenen Schüler, wobei er allerdings nicht nur das in Aussicht gestellte Buch

überreichte, sondern zugleich auch ergänzend bemerkte, daß die Gabe sich aus vom Schulleiter zu vertretenden Gründen leider verzögert habe. Der insoweit behauptete Sachverhalt wird allerdings vom Schulleiter entschieden bestritten, der in der Darstellung des Schulverbandsvorsitzenden eine unzulässige Polemik seines parteipolitischen Gegners sieht.

Grundsätzlich halte ich die Übermittlung der Adressen von Entlaßschülern an den Schulverband zum Zwecke der Übergabe von Buchgeschenken im Hinblick auf das durch die Verfassung gewährleistete Recht der im Schulverband zusammengeschlossenen Gemeinden auf Mitwirkung im Bereich des Volksschulwesens für vertretbar. Ich habe daher auch im vorliegenden Falle insoweit keine Beanstandung ausgesprochen. Allerdings gibt der Fall Anlaß, deutlich zu betonen, daß der Datenempfänger gerade hier an den für die Datenübermittlung maßgebenden Zweck strikt gebunden ist. Gegen eine Nutzung der Daten etwa zu persönlichen Auseinandersetzungen zwischen Schulverbandsvorsitzendem und Schulleiter müßte ich aus datenschutzrechtlicher Sicht Bedenken geltend machen, da der die Datenübermittlung rechtfertigende Zweck in diesem Fall verfehlt würde.

- In einem anderen Falle hatte ich mich mit der Übermittlung von Schülerdaten an Strafverfolgungsbehörden zu befassen. Hier ist darauf hinzuweisen, daß die Staatsanwaltschaft nach § 161 StPO von allen öffentlichen Behörden Auskunft verlangen und Ermittlungen jeder Art entweder selbst vornehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen lassen kann. Auch die Schulen sind daher zur Erteilung von Auskünften im Strafverfahren verpflichtet.

- Befaßt war ich im Berichtszeitraum ferner auch mit Einzelfragen zur Personaldatenverarbeitung. So wollte ein Mitglied einer Personalvertretung von mir wissen, ob es möglich wäre, eine Liste mit den Namen aller Lehrer eines Landkreises, die zur Zeit in der sog. mobilen Reserve eingesetzt sind, zu veröffentlichen. Ergänzend bat er u. a. um Mitteilung, ob die Herausgabe einer entsprechenden Liste an die Personalvertretung zulässig wäre. Beide Fragen habe ich im Benehmen mit dem Staatsministerium für Unterricht und Kultus verneint. Eine gesetzliche Grundlage für die fragliche Datenübermittlung ist nicht ersichtlich. Auch dem Personalrat steht nicht das Recht zu, die fraglichen Personaldaten zu erfragen. Insbesondere besteht kein Mitbestimmungsrecht, das sich allgemein auf die Durchführung des Einsatzes der mobilen Reserve auswirkt.

- Abschließend möchte ich noch auf ein Kompetenzproblem hinweisen, das mich im Berichtszeitraum beschäftigt hat. Im letzten Jahr erreichten mich mehrere Datenschutzregistermeldungen von privaten, staatlich anerkannten Ersatzschulen in kirchlicher Trägerschaft. Im Benehmen mit dem Datenschutzbeauftragten der bayerischen Diözesen im Erzbischöflichen Ordinariat München habe ich die Auffassung vertreten, daß diese Schulen meiner Kontrollkompetenz nicht unterliegen; ihre Meldungen sind demzufolge auch nicht in das bei mir geführte Datenschutzregister aufzunehmen.

  Zwar haben Privatschulen als staatlich anerkannte Ersatzschulen grundsätzlich das öffentliche Schulrecht anzuwenden. Für sie gilt insoweit und damit jedenfalls für Daten von Schülern und Erziehungsberechtigten in der Regel das Bayerische Datenschutzgesetz. Aus verfassungsrechtlichen Gründen haben die Kirchen aber das Recht, ihre Angelegenheiten innerhalb der Schranken des für alle geltenden Gesetzes selbst zu ordnen und zu verwalten. Zu diesen Angelegenheiten gehören nicht nur Fragen des geistlich-religiösen Auftrages der Kirche, sondern auch die Entscheidung darüber, mit welchen Mitteln und in welchen Organisationsformen dieser Auftrag erfüllt wird. Ich teile deshalb die Auffassung, daß sich die Garantie der kirchlichen Selbstbestimmung nicht auf die institutionalisierte Amtskirche und die rechtlich selbständigen Teile dieser Organisation beschränkt, sondern grundsätzlich alle der Kirche zugeordneten Einrichtungen ohne Rücksicht auf die Rechtsform erfaßt, wenn sie nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend berufen sind, ein Stück Auftrag der Kirche in dieser Welt wahrzunehmen und zu erfüllen (vgl. BVerfGE 46, 73).

  Die vielfältigen diakonischen, erzieherischen, publizistischen, missionarischen und sonstigen Aktivitäten, durch die die Kirche ihren Auftrag außerhalb ihrer institutionalisierten Organisation erfüllt, gehören deshalb meines Erachtens verfassungsrechtlich gesehen zur Kirche. Auch privatrechtlich organisierte Schulen in kirchlicher Trägerschaft sind damit kirchliche Einrichtungen, auf die sich das verfassungsrechtlich gewährleistete Selbstverwaltungsrecht erstreckt. Sie sind ebenso wie die Kirche selbst einer Kontrolle durch den staatlichen Datenschutzbeauftragten entzogen.

13. Archivwesen und Forschung

Im Bereich des Archivwesens hat sich im Berichtszeitraum in keinem einzigen Fall ein Anlaß für eine Beanstandung ergeben. Vielmehr habe ich ein erfreuliches Datenschutzbewußtsein und ein ausgeprägtes Verständnis für den Persönlichkeitsschutz festgestellt. Es zeigt sich, daß der Persönlichkeitsschutz im Archivwesen grundsätzlich einer langen Tradition entspricht.

13.1. Archivgesetzgebung

In den Archiven werden große Mengen personenbezogener Daten erfaßt, verarbeitet, ausgewertet und für wissenschaftliche und rechtliche Zwecke nutzbar gemacht. In Zukunft dürften die Archive immer mehr auch mit Daten aus Dateien befaßt werden, die bei den Ausgangsbehörden in automatisierten Verfahren gespeichert und genutzt wurden. Deshalb herrscht allgemeine Übereinstimmung, daß eine bereichsspezifische Regelung der Datenverarbeitung in den Archiven dringend geboten ist. Die Arbeiten zur Vorbereitung eines Bayerischen Archivgesetzes sind im Berichtszeitraum weiter vorangetrieben worden, wobei ich mehrfach Gelegenheit erhielt, Bedenken und Anregungen vorzutragen. Hierfür möchte ich ausdrücklich danken. Inzwischen hat das Staatsministerium für Unterricht und Kultus einen überarbeiteten Ressortentwurf eines Bayerischen Archivgesetzes vorgelegt, der zahlreiche meiner Überlegungen und Anregungen berücksichtigt.

Einige Probleme sind aus datenschutzrechtlicher Sicht noch nicht gelöst:

- Nach dem bisherigen Stand der Diskussion war davon auszugehen, daß das Archivgesetz eine Verpflichtung aller öffentlichen Stellen des Freistaates Bayern enthalten wird, nicht mehr benötigte Unterlagen den staatlichen Archiven zur Übernahme anzubieten. Diese Anbietungspflicht ist in dem neuen Ressortentwurf des Staatsministeriums für Unterricht und Kultus durch eine „Kann Regelung" ersetzt worden. Aus datenschutzrechtlicher Sicht bestehen hiergegen grundsätzlich keine Einwände. Es muß allerdings berücksichtigt werden, daß damit Regelungen auch für das weitere Verfahren bezüglich der Unterlagen geschaffen werden müssen, die den Archiven nicht angeboten, sondern von den Ausgangsbehörden z. B. in eigener Regie archiviert werden. Derzeit enthält der Entwurf hier eine Regelungslücke, die durch das Heranziehen der (subsidiären) Bestimmungen des Bayerischen Datenschutzgesetzes nicht sachgerecht geschlossen werden könnte. So müßten z. B. auch archivwürdige Daten nach Art. 20 Abs. 4 BayDSG auf Verlangen des Betroffenen gelöscht werden.

- Ich halte an meinem Vorschlag fest, den Beginn der (in der Regel 30jährigen) Sperrfrist für die Nutzung der archivierten Daten an den „Abschluß" der Unterlagen durch die Behörden (oder an den Zeitpunkt der Archivierung) zu knüpfen. Ein Anknüpfen an die Entstehung der Unterlagen, wie es der Entwurf derzeit vorsieht, würde zu dem Ergebnis führen, daß die Sperrfrist für alle Unterlagen im Regelfalle bereits im Zeitpunkt der Archivierung längst abgelaufen wäre, weil die Unterlagen der Entwurfsbegründung zufolge den Archiven regelmäßig erst 30 Jahre nach ihrem Abschluß angeboten werden sollen.

13.2. Benutzung von Archivgut für Forschungszwecke

Im Berichtszeitraum haben mich wieder Eingaben erreicht, in denen es um die Möglichkeit der Nutzung von personenbezogenem Archivgut und die hierzu zu erteilenden Auflagen ging. Alle Fälle konnten ohne Beanstandung im Benehmen mit den zuständigen Archivbehörden geklärt werden.

Als Auflage für eine Archivnutzung habe ich wie schon bisher regelmäßig eine Klausel befürwortet, durch die dem Antragsteller aufgegeben wird, rechtzeitig ein Pflichtstück der beabsichtigten Veröffentlichung an die Generaldirektion der Staatlichen Archive Bayerns abzuliefern, damit dieser Behörde die Möglichkeit eröffnet wird festzustellen, ob die weiteren, dem Schutz der Persönlichkeitsrechte Betroffener sowie Dritter dienenden Auflagen eingehalten werden. Auch das Staatsministerium des Innern verbindet, wie mir von dort mitgeteilt wurde, seine Zustimmung zu einer Nutzung von Archivunterlagen aus dem dortigen Geschäftsbereich nach wie vor mit einer solchen Pflichtstückeklausel, sofern sensibles Aktengut eingesehen werden soll. Ich begrüße diese Praxis des Innenministeriums, obwohl ich mir darüber im klaren bin, daß die Generaldirektion der Staatlichen Archive Bayerns mit ihrer beschränkten Personalkapazität kaum in der Lage sein wird, die zahlreichen und oft sehr umfangreichen Veröffentlichungen von Archivnutzern intensiv auf die Verletzung von Persönlichkeitsrechten hin durchzusehen. Unbeschadet dessen messe ich der Klausel auch in Zukunft eine zumindest präventive Wirkung zum Schutz des Persönlichkeitsrechts aller Betroffenen bei.

14. Straßenverkehr

14.1. Zentrales Verkehrsinformationssystem (ZEVIS)

Mit der Novellierung des Straßenverkehrsgesetzes vom 28.1.1987 und dem Inkrafttreten der Fahrzeugregisterverordnung am 29.10.1987 sind die rechtlichen Voraussetzungen für die bundesweite Einführung des Zentralen Verkehrsinformationssystems (ZEVIS) geschaffen worden. Neben den bei den Zulassungsstellen geführten örtlichen Fahrzeugregistern, die Angaben zum zugelassenen Fahrzeug und zum Halter enthalten, wird beim Kraftfahrt-Bundesamt in Flensburg ein zentrales Fahrzeugregister geführt. Mit ZEVIS sind Teile der Dateien des Kraftfahrt-Bundesamtes nun besser nutzbar und außerdem die technischen Voraussetzungen geschaffen, der Polizei online (Direktabruf) die Datenbestände zu erschließen und Auskünfte im einstelligen Sekundenbereich zu erteilen.

Um zu verhindern, daß dieser erleichterte Zugang zu den Dateien des Kraftfahrtbundesamts mißbräuchlich genutzt wird, oder um etwaige mißbräuchliche Nutzungen aufzeigen zu können, werden 2 % aller im Wege des automatisierten Abrufverfahrens erteilten Auskünfte protokolliert. Für die Kontrolle der Abrufe bayerischer Stellen ist der Bayerische Landesbeauftragte für den Datenschutz zuständig. Von diesen Kontrollmöglichkeiten beabsichtige ich demnächst Gebrauch zu machen.

So sehr ich die mit der Novelle des Straßenverkehrsgesetzes und der Fahrzeugregisterverordnung eingeräumten Kontrollrechte begrüße, so wenig kann die Novellierung in gesetzestechnischer Hinsicht befriedigen. Wegen der umfangreichen, schwer lesbaren und wenig verständlichen Bestimmungen, die durch bis ins letzte Detail gehende Regelungen „Normenklarheit" schaffen sollen, ist hier ein für die Verwaltungspraxis nur schwer vollziehbares Gesetz entstanden. Bereichsspezifische Datenschutzregelungen – so notwendig sie im Einzelfall auch sein mögen – dürfen nicht durch derart detaillierte und unüberschaubare Regelungen an den Erfordernissen des Verwaltungsvollzuges vorbeigehen. Durch die Anforderungen des Bundesverfassungsgerichts waren diese detaillistischen Regelungen nicht geboten. Für künftige bereichsspezifische Datenschutzregelungen darf die Novellierung des Straßenverkehrsgesetzes nicht als Vorbild dienen.

14.2. Einzelfälle

Die Novellierung des Straßenverkehrsrechts hat auch Auswirkungen auf die **Datensammlungen der Kfz-Zulassungsstellen**. Insbesondere mit der Fahrzeugregisterverordnung ist der Katalog der von den Zulassungsstellen zu speichernden Daten eindeutig festgelegt. Auch der Umfang der regelmäßigen Datenübermittlungen aus dem örtlichen Fahrzeugregister an andere Stellen, vor allem an Versicherungen, Finanzämter und externe Zulassungsstellen, wird mit Blick auf die jetzt geltenden Vorschriften zu überprüfen sein. Offensichtlich sind diese Rechtsänderungen noch nicht hinreichend bekannt, wie eine kürzlich eingegangene Meldung zur Errichtung einer neuen automatisierten Datei im Kfz-Zulassungswesen gezeigt hat. Deshalb habe ich mich bereits mit dem Staatsministerium für Wirtschaft und Verkehr in Verbindung gesetzt, damit die Kfz-Zulassungsstellen insbesondere beim Einsatz landesweit angebotener automatisierter Verfahren möglichst kurzfristig das neue Straßenverkehrsrecht beachten.

Auch Zulässigkeit und Umfang der sog. **Halterauskünfte** bei den Zulassungsstellen, die immer wieder Gegenstand von Eingaben sind, sind nun mit Inkrafttreten des Gesetzes zur Änderung des Straßenverkehrsgesetzes geklärt. So dürfen nach § 39 Straßenverkehrsgesetz Halterdaten zur Verfolgung privater Rechtsansprüche nur noch übermittelt werden, wenn das Interesse des Datenempfängers auf einem Vorgang im Straßenverkehr beruht.

In Fällen, in denen Automobilhersteller oder -importeure Auskünfte über Zulassungs- und Abmeldedaten oder Besitzumschreibungen wünschen, um die Einhaltung ihrer mit Händlern oder Großabnehmern getroffenen vertraglichen Abmachungen über Absatz und Verwendung bestimmter Fahrzeuge überprüfen zu können, ist ein Bezug zum Straßenverkehr nicht gegeben. Personenbezogene Auskünfte in Angelegenheiten dieser Art dürfen deshalb jedenfalls künftig nicht mehr erteilt werden. In dieser Beurteilung bin ich mit dem Staatsministerium für Wirtschaft und Verkehr einig, das mittlerweile die Bezirksregierungen und Kreisverwaltungsbehörden angewiesen hat, entsprechend zu verfahren.

Im Berichtszeitraum haben sich mehrfach Bürger an mich gewandt, die, wie sich bei meiner Prüfung jeweils herausstellte, auf Grund von **Verwechslungen bei der Halterfeststellung** zu Unrecht einer Verkehrsordnungswidrigkeit beschuldigt worden sind. Einem Bürger ist dies allein dreimal in einem Jahr passiert. Meine Ermittlungen in diesen Fällen haben ergeben, daß diese Verwechslungen zum Teil auf Erfassungsfehlern beruht haben. Allerdings war ein Teil der Verwechslungen auch darauf zurückzuführen, daß das zur Halterfeststellung eingeschaltete Kraftfahrtbundesamt zwischenzeitlich eingetretene Veränderungen hinsichtlich des Halters eines Kraftfahrzeugs trotz rechtzeitiger Meldung der bayerischen Zulassungsstellen in seinen Dateien noch nicht berichtigt hatte. In einem Fall war der Halterwechsel sogar mehr als ein Jahr zurückgelegen. Soweit derartige Verwechslungen allerdings darauf zurückzuführen sind, daß bei der örtlichen Zulassungsstelle vorliegende Vermerke über Löschungen oder Stillegungen eines Kraftfahrzeugs von der für die Verkehrsordnungswidrigkeiten zuständigen Polizeidienststelle aus programmtechnischen Gründen nicht übernommen werden, müssen entsprechende organisatorische Maßnahmen getroffen werden. Um die durch derartige Verwechslungen entstehenden unnötigen Belastungen für die Bürger künftig weitestmöglich zu vermeiden, werde ich den möglichen Fehlerquellen weiter nachforschen und gegebenenfalls auf entsprechende Änderungen drängen.

15. Industrie- und Handelskammern

15.1. Datenerhebung durch die IHK für das Handelsregister

Aufgrund einer Beschwerde über die Datenerhebung durch eine Industrie- und Handelskammer (IHK) hatte ich mich mit folgendem Sachverhalt zu befassen: Neben Daten, die die IHK für eigene Zwecke benötigt, erhebt sie auch Daten zur Feststellung, ob Gewerbetreibende zum Handelsregister anzumelden sind. Die IHK unterstützt damit nach § 1 Abs. 1 und Abs. 4 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern und nach § 126 des Gesetzes über die freiwillige Gerichtsbarkeit das Registergericht. Die zwangsweise Erhebung von Daten ist allerdings dem Registergericht selbst vorbehalten. Die Kammern können die Daten nur erheben, wenn die Gewerbetreibenden freiwillig mitwirken oder ein Ersuchen des Registergerichts um gutachtliche Stellungnahme vorliegt.

Nach Beratung mit dem Landesbeauftragten für den Datenschutz weisen die Industrie- und Handelskammern nunmehr auf die Freiwilligkeit der erbetenen Angaben ausdrücklich hin.

Bei dieser Gelegenheit wurde der Erhebungsbogen so ergänzt, daß der Ausfüllende sein Einverständnis mit der Weitergabe personenbezogener Daten an die Handwerkskammer erklärt, wenn sich aus der Beantwortung ergibt, daß eine Eintragung in die Handwerksrolle besteht oder beantragt ist.

15.2. Aufbau einer bundesweiten IHK-Informationsdatenbank

Eine Industrie- und Handelskammer hat mich über den beabsichtigten Aufbau einer bundesweiten Produktdatenbank informiert, welche die Grundlage bei Geschäftsanbahnungen und Herstellernachweisen bilden soll, und um datenschutzrechtliche Würdigung gebeten. Die Produktdatenbank soll den Unternehmen des produzierenden Gewerbes die Möglichkeit bieten, ihr gesamtes Fertigungsprogramm erfassen zu lassen, die für eine Geschäftsanbahnung wichtigen Firmendaten interessierten Geschäftskreisen und weiteren potentiellen Interessenten zugänglich zu machen und sich so neue Absatzchancen zu eröffnen. Die erforderlichen Daten sollten in einer Fragebogenaktion bei allen kammerzugehörigen Betrieben erhoben werden.

Meine Vorschläge zur datenschutzgerechten Gestaltung der Fragebogen und zur daran anknüpfenden Datenverarbeitung (deutlicher Hinweis auf die Freiwilligkeit, Einwilligung in die Datenspeicherung und Datenübermittlung, Aufklärung der Betroffenen über die Bedeutung der Einwilligung und des Verfahrens) wurden in das Verfahren eingebezogen, so daß keine Bedenken gegen den Aufbau der Produktdatenbank bestehen.

16. Neue Medien

Auf dem Gebiet der Neuen Medien, also bei Bildschirmtext, der Anwendung des Medienerprobungs- und -entwicklungsgesetzes, des Fernwirksystems Temex (Fernmessen, Fernanzeigen und Fernschalten) und der Telekommunikationsordnung sind im Berichtszeitraum keine besonderen datenschutzrechtlichen Probleme entstanden. Dies liegt zum einen darin begründet, daß für Bildschirmtext und die Mediendienste in Bayern bereichsspezifische Datenschutzregelungen bestehen, und zum anderen in den nach wie vor geringen Teilnehmerzahlen.

16.1. Bildschirmtext

Die Überwachung der Einhaltung der Datenschutzvorschriften des Bildschirmtext-Staatsvertrags bei öffentlichen Stellen ist nach Art. 1 Abs. 2 Ausführungsgesetz zum Bildschirmtext-Staatsvertrag dem Landesbeauftragten für den Datenschutz zugewiesen. Meine stichprobenartigen Kontrollen der Bildschirmtextangebote öffentlicher Stellen

haben im Berichtszeitraum zu keiner Beanstandung geführt. Soweit Bürger Datenschutzverstöße privater Stellen mitgeteilt haben, habe ich die Eingaben an die zuständigen Aufsichtsbehörden abgegeben. Von der im Ausführungsgesetz zum Bildschirmtext Staatsvertrag ausdrücklich vorgesehenen Möglichkeit, mich zu Kontrollen auch im privaten Bereich zu beauftragen oder mich hierbei einzuschalten, haben die Aufsichtsbehörden keinen Gebrauch gemacht.

Gutachtlich bin ich allerdings mit folgender Fragestellung befaßt gewesen: Einzelne Anbieter stellen in Bildschirmtext eine Angebotsseite – eine sogenannte Pinnwand – zur Verfügung, die jeder Teilnehmer gegen Gebühr für eigene Mitteilungen im Bildschirmtextsystem nutzen kann. In zahlreichen Fällen wird eine solche – allen Teilnehmern zum Abruf zugängliche – „Pinnwand" für Inhalte obszöner Art genutzt. In einem Fall ist eine Lehrerin wohl Ziel eines üblen Schülerstreiches geworden, weil deren Telefonnummer mit der Aufforderung, „heiße" Telefongespräche zu führen, auf einer solchen Seite eingestellt war. Die Teilnehmer, die eine „Pinnwand" für solche Mitteilungen nutzen, bleiben in aller Regel anonym und können deshalb weitgehend ohne eigenes Risiko schutzwürdige Belange Dritter verletzen. Um dies für die Zukunft auszuschließen, habe ich vorgeschlagen, Teilnehmer, die eine „Pinnwand" zur Informationsverbreitung nutzen, als „Unteranbieter" zu behandeln und folglich den für Anbieter geltenden Verpflichtungen des Bildschirmtext-Staatsvertrags zu unterwerfen. Die Nutzer einer „Pinnwand" müßten somit als „Unteranbieter" persönlich erkennbar sein und könnten nicht mehr im Schutz der Anonymität schutzwürdige Belange Dritter beeinträchtigen.

16.2. Telekommunikationsdienste

Die Telekommunikationsordnung, die die Benutzungsbedingungen und -gebühren für die alten (Telefon, Telex) und die neuen Telekommunikationsdienste (z. B. Fernwirkdienste, Textkommunikation, Breitbandverteildienste, Übermittlung von Rundfunkprogrammen) regelt, wird zum 1.1.1988 in Kraft treten. Die Nutzung der neuen Telekommunikationsdienste fällt in die Gesetzgebungskompetenz der Länder. Zu den datenschutzrechtlichen Fragen habe ich deshalb Stellungnahmen abgegeben. Inwieweit in der Praxis tatsächlich datenschutzrechtliche Probleme auftreten, werde ich nach Inkrafttreten der Telekommunikationsordnung prüfen.

16.3. Medienerprobungs- und -entwicklungsgesetz (MEG); Datenschutzfragen in der Praxis

Zweck des Medienerprobungs- und -entwicklungsgesetzes (MEG) ist es, die Nutzung der modernen Breitbandkabel- und Satellitentechnik in geordnete Bahnen zu lenken. In Anlehnung an den Bildschirmtext-Staatsvertrag der Länder wurde der besonderen Gefahrenlage, die aus den neuen Techniken für den Persönlichkeitsschutz des einzelnen Teilnehmers folgen kann, mit der Aufnahme einer eigenen Bestimmung über den Datenschutz in den Gesetzestext Rechnung getragen. Abweichend von den allgemeinen Datenschutzgesetzen ist nach Art. 19 MEG die Zulässigkeit des Abfragens und der Verarbeitung personenbezogener Teilnehmerdaten stärker eingeschränkt. Die Überwachung des Datenschutzes bei der Landeszentrale für Neue Medien, sowie bei Kabelgesellschaften und den Betreibern von Kabelanlagen obliegt dem Landesbeauftragten für den Datenschutz.

Datenschutzrechtliche Prüfungen bei den meiner Kontrolle unterliegenden Stellen habe ich im Berichtszeitraum noch nicht durchgeführt. Sie stehen aber in Kürze an.

Im Berichtszeitraum war ich allerdings mehrfach mit Datenschutzfragen zur Übermittlung von Namen, Inhaber- und Beteiligungsverhältnissen von Rundfunkanbietern befaßt:

- Eine Kabelgesellschaft wurde von einem Kommunalpolitiker um Mitteilung der Inhaber- und Beteiligungsverhältnisse aller für sie tätigen Anbieter gebeten.

  Art. 29 Abs. 1 MEG, der zur Begründung für dieses Auskunftsverlangen herangezogen worden ist, greift jedoch nicht. Nach Art. 29 Abs. 1 Satz 1 MEG ist der Anbieter zwar verpflichtet, am Ende seiner Sendezeit sein „Impressum", also den Namen und die Anschrift des Anbieters und den verantwortlichen Redakteur zu benennen. Die Regelung dient der Sicherung der Rechtsverfolgung Betroffener gegenüber den Anbietern sowie der Offenheit des Meinungsbildungsprozesses. Sie ist auf eine bestimmte, nämlich die gerade beendete Sendung bezogen. Abstrakte Auskunftsverlangen ohne zeitlichen oder inhaltlichen Bezug zu einer Rundfunksendung sind darauf nicht zu stützen.

  Nach Art. 29 Abs. 1 Satz 2 MEG muß die Landeszentrale die Inhaber- oder Beteiligungsverhältnisse des Anbieters und deren Änderung auf schriftliches Verlangen hin mitteilen. Die Landeszentrale erfüllt damit teilweise Aufgaben eines öffentlichen Registers, bei dem betroffene Teilnehmer diejenigen Informationen erhalten sollen, die sie zu ihrer Rechtsverfolgung benötigen. Diese besondere Aufgabe der öffentlich-rechtlich organisierten Landeszentrale kann jedenfalls nicht dergestalt auf private Kabelgesellschaften übertragen werden, daß daraus ein Auskunftsanspruch abgeleitet werden kann. Mangels besonderer Regelung bemißt sich demnach die Offenbarung von Namen, Inhaber- und Beteiligungsverhältnissen von Anbietern durch Kabelgesellschaften nach § 24 Bundesdatenschutzgesetz. Um die „schutzwürdigen Belange" der Anbieter zu wahren, kann es sich im Regelfall empfehlen, diese vor Weitergabe ihrer Namen nach eventuellen Einwendungen zu befragen. Ergeben sich sodann keine Anhaltspunkte für eine mögliche Beeinträchtigung schutzwürdiger Belange der Anbieter, ist eine Weitergabe von „Impressumsdaten" zulässig.

- Eine andere Kabelgesellschaft wandte sich an mich mit der Frage, ob für sie eine „rechtsverbindliche Auskunftspflicht" bestehe, Dritten Auskünfte über solche Anbieter zu erteilen, die gerade Rundfunkangebote eingereicht haben.

  Eine solche Auskunft**spflicht** besteht nicht. Die Zulässigkeit der Auskunftserteilung richtet sich auch hier nach § 24 BDSG. Im Hinblick auf die notwendige Wahrung der schutzwürdigen Belange im Einzelfall empfiehlt sich auch für diesen Fall die Rückfrage bei den Anbietern.

- Die Bayerische Landeszentrale für Neue Medien (BLM) war gebeten worden, sämtliche Inhaber- und Beteiligungsverhältnisse einer bestimmten Kabelgesellschaft auf eine Anfrage hin zu offenbaren. Eine solche Anfrage

löst einen erheblichen Ermittlungsaufwand über etwaige gesellschaftsrechtliche Verflechtungen aus. Die Landeszentrale wollte die Auskunftserteilung nur auf einen Anbieter beschränken und das Ersuchen nur berücksichtigen, wenn ein „berechtigtes Interesse" dargelegt werde.

Um Stellungnahme gebeten, teilte ich der BLM mit, daß ich ihre Auffassung insoweit teile, als die Mitteilungspflicht der BLM nach dem deutlichen Wortlaut des Art. 29 Abs. 1 Satz 2 MEG auf einen konkret benannten Anbieter beschränkt ist. Die BLM ist nicht zu „Sammelauskünften" verpflichtet. Allerdings ist der Nachweis des „berechtigten Interesses" keine gesetzliche Voraussetzung für die Erteilung derartiger Auskünfte durch die BLM. Dafür findet sich kein Anhaltspunkt im Gesetzeswortlaut. Zwar muß die BLM bei der Auskunftserteilung neben dem Informationsbedürfnis der Öffentlichkeit auch das allgemeine Persönlichkeitsrecht Betroffener berücksichtigen, doch hat die Landeszentrale die Möglichkeit, die Angaben etwa auf den Umfang einer Handelsregisterauskunft zu beschränken. Einer solchen Auskunft dürften im Regelfall weder schutzwürdige Anbieterbelange entgegenstehen, noch dürfte sie eine unzumutbare Belastung für die Landeszentrale bedeuten.

- Anläßlich einer Eingabe eines Bürgers erhielt ich davon Kenntnis, daß die Bayerische Landeszentrale für Neue Medien regelmäßig die zuständige Kabelgesellschaft über den Betrieb auch von privaten Individual-Satelliten-Empfangsanlagen in Kenntnis setzt, die ausschließlich dem eigenen Rundfunkempfang dienen.

  Derartige Übermittlungen wären nach dem Bayerischen Datenschutzgesetz nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der BLM zugewiesenen Aufgaben erforderlich sind oder die Kabelgesellschaft ein berechtigtes Interesse an der Kenntnis des privaten Betreibers der Anlage glaubhaft macht und dadurch schutzwürdige Belange des Betreibers nicht beeinträchtigt werden. Weder das MEG noch sonstige Rechtsnormen weisen der Landeszentrale die Aufgabe zu, Kabelgesellschaften über Individual-Satelliten-Empfangsanlagen zu unterrichten; der Individualempfang löst auch keine Entgeltsansprüche der Kabelgesellschaften aus. Die Übermittlungen sind unzulässig. Die BLM hat inzwischen erklärt, künftig auf solche Datenübermittlungen an Kabelgesellschaften zu verzichten.

17. Technischer und organisatorischer Bereich

17.1. Technische Grundsatzfragen

17.1.1. Sicherheit von Personal Computern

In früheren Tätigkeitsberichten wurde ausführlich über diese Thematik berichtet. An dieser Stelle soll noch einmal ein Resümee gezogen werden, ob und wie sich die Sicherheit der Datenverarbeitung auf Personal Computern erhöht hat.

Personal Computer sind persönliche Rechner, die die Rechnerleistung unmittelbar an den Arbeitsplatz des Endbenutzers bringen. Anders als bei der Datenverarbeitung auf Großrechnern und Systemen mittlerer Größe kann hier der Benutzer Bediener, Systemprogrammierer, Dateiverwalter, Programmierer und Sachbearbeiter in einer Person sein. Das in der Groß-EDV geläufige Sicherungsprinzip der Funktionstrennung greift beim Einsatz von Personal Computern nicht. Die Datensicherheit muß deshalb auf andere Weise gewährleistet werden.

Erfreulich aus der Sicht des Datenschutzes ist, daß bei einem PC-Einsatz auch der Datensicherheit heute mehr Bedeutung beigemessen wird als früher. Nicht zuletzt das wachsende Problembewußtsein der Anwender hat die Hersteller dazu veranlaßt, nunmehr auch die Sicherheit unterstützende Hard- und Softwareprodukte anzubieten. Diese positive Entwicklung wurde letztlich auch dadurch begünstigt, daß die Personal Computer, die ursprünglich Einplatzsysteme waren, sich zunehmend – sieht man von den sogenannten Homecomputern ab – zu Mehrplatzsystemen entwickeln. Schließlich stehen technische Einrichtungen, sogenannte Netzwerke zur Verfügung, die es gestatten, mehrere Geräte miteinander zu vernetzen. Von der Vernetzung der Personal Computer wird im öffentlichen Bereich allerdings kaum Gebrauch gemacht.

Auch bei den Speichern werden Größenordnungen erzielt, die noch vor Jahren undenkbar erschienen. Festplattenspeicher erreichen heute bereits Größenordnungen von 100 Megabyte (MB) und neben den Disketten hat sich das leistungsfähigere Streamer-Tape, das Speicherkapazitäten bis zu 90 MB erreicht, bereits im Professional-Bereich durchgesetzt. Das Streamer-Tape wird häufig zur Datensicherung verwendet. Wegen der Möglichkeit, große Datenmengen speichern zu können, werden zur Sicherung der Hardware Spezialschränke eines hohen Sicherheitsstandards angeboten.

Zunächst wurden die Anforderungen der Datensicherheit und Zugriffssicherung bei der Entwicklung der Betriebssysteme für Personal Computer vernachlässigt. Mittlerweile ist jedoch auch hier ein Trend zu größerer Sicherheit zu beobachten. So gibt es für das marktbeherrschende Single-User-Betriebssystem MS-DOS (Microsoft Disk-Operating-System der Fa. Microsoft) eine Reihe von Produkten, die hardware- oder softwaremäßig den Zugriffsschutz unterstützen. Damit wird auch der Multi-User-Betrieb datenschutzrechtlich vertretbar. Zu erwähnen sind hier vor allem die Produkte, die Daten und Programme verschlüsseln, so daß einem Fremden, der den Entschlüsselungscode nicht kennt, die gespeicherten Ursprungsinformationen nicht zugänglich sind. Die Version 2 des MS-DOS, die im Jahre 1983 ausgeliefert wurde, enthält die Möglichkeit des Aufbaus eines hierarchischen Dateisystems und zusätzliche Security-Funktionen. Auch die allgemeine Datensicherung wurde ab dieser Version besser unterstützt. Mit der Einführung der Version 3 des MS-DOS erlangte das System die Mehrbenutzer- und die Netzwerkfähigkeit. Schließlich ist geplant, in der Version 5 des MS-DOS auch die Mehrplatzfähigkeit zu unterstützen. Das wird neue Überlegungen zur Datensicherheit erforderlich machen.

Das Betriebssystem UNIX, das in den USA von BELL erstmals für den Minicomputer DEC PDP/11 der Digital Equipment Cooperation entwickelt wurde, enthält bereits standardmäßig die aus der Groß-EDV bekannten Zugriffschutzmechanismen über Benutzeridentifikation und Paßwort. Auch hier bieten Fremdfirmen Produkte, etwa Verschlüsselungsprogramme an, die die Datensicherheit der von UNIX verwalteten Datenbestände noch erhöhen.

Von den einschlägigen Fachgremien wurden bislang keine Mindestanforderungen an die Sicherheit und Transparenz der Nutzung von Kleinrechnern definiert. Auch die Typprüfung mit einem Sicherheitssiegel, angeregt durch die Gütegemeinschaft Software (GGS), konnte sich nicht durchsetzen.

In der Zukunft wird es für die Datensicherung wichtig sein, daß zumindest bei größeren Institutionen eine Person damit beauftragt wird, den Einsatz der Personal Computer zu kontrollieren. Da diese Geräte auch in absehbarer Zukunft nicht über Protokollierungseinrichtungen verfügen werden, die die getätigten DV-Aktivitäten dokumentieren, ist auf die Einhaltung der vorgegebenen organisatorischen Sicherheitsmaßnahmen (Dokumentation der ablaufenden Aufgaben und der Benutzer) ganz besonders großer Wert zu legen.

17.1.2. Sicherheit von Kommunikationsnetzen (Hacker-Problematik)

Von Zeit zu Zeit wird in den Medien darüber berichtet, daß Unbefugte in fremde Computersysteme eindrangen und dort von geheimen Informationen Kenntnis erhielten. 1987 war ein bedeutender amerikanischer Computerhersteller betroffen. Die Eindringlinge sollen nachgewiesen haben, daß ihnen Fehler im Betriebssystem den Zugang zum Rechnersystem ermöglichten. Viele dieser Eindringlinge, auch Hacker genannt, sehen angeblich ihre Aufgabe darin, Systemfehler aufzudecken und Schwachstellen im Sicherheitssystem ausfindig zu machen, damit die DV-Systeme sicherer werden. Der Hersteller hat mittlerweile reagiert und eine neue Betriebssystemversion ausgeliefert, in der diese Fehler behoben sein sollen. In der bayerischen Verwaltung werden DV-Anlagen dieses Typs allerdings nicht eingesetzt, so daß kein Grund zur Aufregung bestand.

Grundsätzlich ist hierzu jedoch zu bemerken, daß ein Eindringen in einen Fremd-Computer nur dann möglich ist, wenn dieser über entsprechende Anschlußstellen verfügt. Sind keine Anschlußstellen vorhanden, ist ein Eindringen nicht möglich. Wegen der zunehmenden Bedeutung der Datenfernverarbeitung verfügen heute allerdings nahezu alle bedeutenden Rechner über Verbindungen zu entfernten Benutzern des DV-Systems. Als Transportmedium für die Daten von und zum zentralen Rechner dienen Leitungen, die in der Bundesrepublik die Deutsche Bundespost zur Verfügung stellt. Der Benutzer kann zwischen festen und im Bedarfsfall geschalteten Verbindungen wählen. Im einen Fall spricht man von Standleitungen, im anderen von Wählleitungen. Während Standleitungen ein geschlossenes System kennzeichnen, kann über Wählleitung im Prinzip jedermann, der die Anwahlnummer kennt, mit dem Zentralrechner in Verbindung treten. Ob freilich in einem solchen Falle ein Dialog mit dem Rechner zustande kommt, hängt davon ab, ob sich der Anwählende als Berechtigter ausweisen kann. Besitzt er eine gültige, dem Rechner bekannte Benutzerkennung und das dafür vereinbarte Paßwort, akzeptiert ihn das System. Er kann im Rahmen der vereinbarten Aktivitäten auf dem System arbeiten und auf dort gespeicherte Daten zugreifen.

Manche dieser in fremde Rechnersysteme mißbräuchlich eindringende Personen versuchen, gültige Benutzerkennungen auszuspähen oder durch Probieren herauszubekommen. Besonders leicht macht man es, wird auf den Schutz durch Paßworte verzichtet. Gelangt ein Hacker in den Besitz der Benutzerkennung eines privilegierten Benutzers, beispielsweise des Systemprogrammierers, stehen ihm im System alle Möglichkeiten offen, sofern er über genügende Systemkenntnisse verfügt.

Durch zusätzliche Sicherheitseinrichtungen wie die Rückrufautomatik, lassen sich aber auch Wählleitungen sicherer machen. Beim Einsatz der Rückrufautomatik wird nach der Identifikation des Anrufenden die Verbindung getrennt und das für die Kennung vereinbarte Endgerät von der Zentrale aus direkt angewählt. Ein Hacker hat dann von seinem Ausgangspunkt keine Chance, mit dem Rechner in Verbindung zu treten, weil im Rechner der Hackeranschluß natürlich nicht bekannt ist. Die Rückrufautomatik verursacht allerdings zusätzliche Kosten, so daß bislang von ihr nur in Ausnahmefällen Gebrauch gemacht wird.

Wählanschlüsse sind auch dann sicher, wenn sie nur von der Zentrale aus aktiviert werden, wie das im Netz der Anstalt für Kommunale Datenverarbeitung in Bayern der Fall ist, wenn die Zentrale in der Nacht die Daten bei den angeschlossenen Kunden abruft.

Schließlich existieren in den Rechenzentren Wählanschlüsse zur Durchschaltung an die Wartungszentrale beim Hersteller. Auch hier geht die Initiative meist von der Zentrale aus. Zudem bietet die Deutsche Bundespost für ein geringes Entgelt einen Spezial-Fernsprechapparat an, in dem bestimmte Rufnummern eingegeben werden können, zu denen eine Verbindung hergestellt werden soll. Ein Verbindungsaufbau zu anderen Endgeräten ist damit ausgeschlossen.

In Bayern gibt es in der Datenverarbeitung durch öffentliche Stellen keine Anzeichen dafür, daß Hacker ohne Mitwirkung eines Komplizen in den Zentralrechner eindringen können.

Eine Manipulation an den Verbindungsleitungen ist theoretisch zwar möglich, aber praktisch wenig wahrscheinlich, da die Deutsche Bundespost ein anonymes Netz betreibt. Der Leitung sieht man es nicht an, woher sie kommt und wohin sie führt. Durch Abhören einer Leitung ließe sich der Dialog aufzeichnen. Der Abhörende käme dann in den Besitz der ausgetauschten Informationen, sofern er sie entschlüsseln kann. Ein Durchtrennen der Leitung und der Anschluß eines fremden Endgerätes würden in den meisten Fällen jedoch zu einer Störung führen und vom Netzbetreiber erkannt werden.

Bisher bestand kein Anlaß, die Datenfernverarbeitung einer Behörde wegen mangelnder Sicherheit zu beanstanden.

17.1.3. „Kompromittierende" Abstrahlung

Anwender und Betreiber von DV-Anlagen werden wegen der in der Fachpresse immer häufiger zu findenden Berichte über die Auswirkungen der kompromittierenden Abstrahlung elektronischer Geräte zunehmend verunsichert. Die kompromittierende Abstrahlung, die beim Transport elektrischer Ladung in Leitungen, Bildschirmen und elektromagnetischen Bauelementen entsteht, ist zwar dem Fachmann seit langem bekannt, ihre Bedeutung, die sie für die Sicherheit von weitverzweigten DV-Systemen hat, wurde bislang allerdings stets vernachlässigt. In den letzten zwei Jahren machten aufsehenerregende Versuche, in denen gezeigt wurde, wie einfach Bildschirminhalte durch Verwertung der Abstrahlung drahtlos auf einem geeigneten Empfangsgerät sichtbar gemacht oder gespeichert werden können, den

Verantwortlichen in der Datenverarbeitung die Problematik der Abstrahlung bewußt.

Besonders intensiv „strahlen" Bildschirme. Starke Signale, hervorgerufen durch die Steuerung der Mechanik, wurden unter anderem auch bei Typenraddruckern, Fernschreibern und elektrischen Kugelkopfschreibmaschinen gemessen. Hingegen ist die kompromittierende Abstrahlung der Zentraleinheit sowie der Magnetband- und Magnetplattengeräte des Hostrechners zu vernachlässigen. Bei den Leitungen ist die Abstrahlung bei einfachen Kabeln und Zwei-Draht-Leitungen am größten. Mehradrige Kabel, Koaxialkabel und Glasfaserkabel gelten weitgehend als abstrahlsicher.

Während bei Leitungen die Abstrahlung nur bis zu einem Abstand von wenigen Metern verwertbar ist, kann die Abstrahlung von Bildschirmen und Druckern noch in einer Entfernung von einigen hundert Metern nachgewiesen werden. Wegen der unterschiedlichen Charakteristik der Bildschirmröhren ist zudem die gegenseitige Störung der von verschiedenen Bildschirmen ausgehenden Strahlung gering, so daß die von bis zu 20 verschiedenen Bildschirmen ausgehende kompromittierende Abstrahlung getrennt erfaßt werden konnte.

Die VDE-Bestimmungen 0846 ff (VDE – Verein deutscher Elektroingenieure) befassen sich zwar mit Emissionen aus DV-Geräten und mit der Störanfälligkeit von DV-Geräten, Grenzwerte für die kompromittierende Abstrahlung enthalten diese Richtlinien jedoch nicht. In VDE 0871 ist die zulässige elektrische Feldstärke, die ein Gerät abgeben darf, festgelegt. Sie ist maßgebend, ob ein DV-Gerät vom Fernmeldetechnischen Zentralamt der Deutschen Bundespost (FTZ) zugelassen wird oder nicht. Die Begriffe „abstrahlarm" und „Abstrahlsicherheit" sind in VDE 0871 nicht definiert. Bei der Ermittlung der Stärke der Abstrahlung kann im Einzelfall die Zentralstelle für Chiffrierwesen in Köln (ZfCh) zu Rate gezogen werden. Mir stehen keine technischen Hilfsmittel zur Verfügung, Messungen durchzuführen.

Die Hersteller von DV-Anlagen bemühen sich, kostengünstige abstrahlarme Bildschirme, sogenannte TEMPEST-Bildschirme (temporary emanation and spurious transmission) zu entwickeln. Einige Hersteller vertreiben bereits abstrahlsichere Bildschirme, deren Kosten jedoch ein Vielfaches von dem betragen, was für Standardbildschirme aufzuwenden ist.

Die Nutzung der kompromittierenden Abstrahlung ist auch dadurch zu verhindern, daß man die Räume abschirmt, in denen sich Geräte befinden, die eine Abstrahlung aussenden. Die Kosten für solche Raumschirmungsmaßnahmen sind jedoch beträchtlich. Zur Raumschirmung werden in erster Linie Kupferfolien verwendet. Besonders wichtig ist, auf eine lückenlose Abschirmung zu achten. Es genügt nicht, nur Wände, den Boden und die Decke eines Raumes mit Kupferfolien auszukleiden. Die Schirmung eines Raumes bestimmt letztlich das schwächste Glied in der Kette, und das sind Fenster, Türen, Leitungsschächte und Versorgungsleitungen. Während sich Leitungsschächte und Versorgungsleitungen durch sogenannte Hochfrequenzfilter relativ problemlos abschirmen lassen, bereitet die Abschirmung der Fenster und Türen häufig große Sorgen. Sogenannte Kontaktmesser und Kontaktfedern dienen zur hochfrequenten Schließung von Fenstern und Türen.

Die Kosten für einen abgeschirmten Raum bewegen sich je nach Größe, Anzahl der Türen, der Fenster und der Anzahl der abzuschirmenden Leitungen zwischen 150000.– und 300000.– DM.

Bildschirme lassen sich schließlich in ähnlicher Art umrüsten. Manchmal kann bereits ein Bespannen des Sichtfensters mit einem Kupferdrahtgeflecht eine genügende Dämpfung der kompromittierenden Abstrahlung bewirken.

Die Raumschirmungsmaßnahmen schützen nicht nur gegen Emissionen, sondern auch gegen Immissionen, etwa gegen Strahlenangriffe.

Während meiner Kontrolltätigkeit ist mir allerdings nur ein Fall bekannt geworden, in dem ein Anwender die kompromittierende Abstrahlung eines DV-Gerätes messen ließ. Da bei diesem Gerät die kompromittierende Abstrahlung noch in einer Entfernung von einigen hundert Metern nachgewiesen werden konnte und auf der Anlage sensitive Daten verarbeitet werden sollten, wurde dieses Gerät gegen ein abstrahlungsärmeres System ausgetauscht.

Ganz besonderes Aufsehen erregte es, als kürzlich bekannt wurde, daß Telefonapparate mit eingebauten Gebührenzählern die über sie geführten Telefongespräche in Form von kompromittierender Abstrahlung aussenden. Die Strahlung konnte mit einem gewöhnlichen Radioempfänger in einer Entfernung bis zu einem Meter in ihre akustischen Ursprungswerte zurückgewandelt werden. Hier sind insbesondere die Hersteller aufgerufen, Bauteile zu entwickeln, die keine derartigen Nebeneffekte hervorrufen. Besondere, meist aufwendige Abschirmungsmaßnahmen vom Anwender zu verlangen, widerspräche dem Grundsatz der Verhältnismäßigkeit.

17.1.4. Revision der automatisierten Datenverarbeitung

Die Revision der automatisierten Datenverarbeitung ist nicht nur für die behördeninterne Kontrolle sondern auch für die Personen von großer Bedeutung, die von außerhalb mit der Kontrolle der Einhaltung der Datenschutzregelungen befaßt sind. Dieses Thema wurde zwar bereits in früheren Tätigkeitsberichten behandelt. Da jedoch auch im Berichtszeitraum bei Prüfungen der Revisionsfähigkeit der automatisierten Datenverarbeitung die vorgelegten Unterlagen Mängel aufwiesen, möchte ich an dieser Stelle einige grundlegende Anmerkungen machen.

Für die Revision der maschinellen Datenverarbeitung muß anhand von Unterlagen erkennbar sein, wer, wann, mit welchen Mitteln auf welche Daten zugegriffen hat und wer, wann, welche Zugriffsberechtigungen besaß.

Grundlagen dafür, diese Fragestellungen zu beantworten, sind

- die Dokumentation der Zugriffsrechte aller Benutzer,
- ein Terminplan für alle regelmäßig wiederkehrenden und auf der DV-Anlage abzuwickelnden Aufgaben sowie
- revisionsfähige Aufzeichnungen (Protokolle) über alle auf dem DV-System abgelaufenen Aufgaben.

Diese Unterlagen sind zweckmäßigerweise DV-gestützt, also von außen unbeeinflußbar, zu erstellen und im DV-System zu führen. Großer Wert ist schließlich auch darauf zu legen, daß die lückenlose Abfolge der

aufgezeigten Daten und bei Zugriffsberechtigungen deren Gültigkeitsdauer ersichtlich sind.

Aus Ablaufprotokollen sollen in erster Linie Abweichungen, z.B. die unerlaubte Nutzung eines berechtigten Benutzers, vom ordnungsgemäßen Betrieb des DV-Systems und die Tatsache entnommen werden, daß alle DV-Aufgaben, wie vorbereitet, termingerecht gestartet und beendet wurden.

Anwender mittlerer dezentraler DV-Systeme sind häufig überfordert, diesen Anforderungen der Revision gerecht zu werden. Deshalb wird meine Dienststelle Orientierungshilfen erstellen, die es den Betreibern solcher DV-Systeme erleichtern, den Anforderungen der Revision gerecht zu werden. Dazu sind, wegen der Vielfalt der eingesetzten Hardware-Systeme, noch eine Reihe von Gesprächen mit den Herstellern zu führen. Schließlich darf auch der Blick für die Praxis nicht verlorengehen. Revision darf nicht um ihrer selbstwillen betrieben werden und dazu führen, daß der Verwaltungsaufwand unverhältnismäßig hoch und die Datenverarbeitung behindert wird. Sofern die Hersteller noch keine geeigneten Werkzeuge zur Verfügung stellen, wird man sich in der Übergangszeit auch mit manuellen Aufzeichnungen zufrieden geben müssen.

In der Datenverarbeitung mit Großrechnern bei der die Zahl der Benutzer und der täglich ablaufenden Aufgaben um ein Vielfaches höher liegt als bei den oben geschilderten mittleren dezentralen Systemen, kann man jedoch auf die DV-gestützte Erstellung der Unterlagen für die Revision sicher nicht verzichten. Dieses Anliegen wurde wiederholt an die entsprechenden Hersteller herangetragen. Leider sind die revisionsunterstützenden Softwarekomponenten meist nicht in das Betriebssystem integriert, so daß die Zwangsläufigkeit ihres Einsatzes nicht gegeben ist. Hier ist der Anwender aufgefordert, von den Herstellern Unterstützung zu verlangen. Die meisten Hersteller haben dieses Anliegen erkannt.

17.2. Prüfungstätigkeit

Mit der Prüfung der technischen und organisatorischen Maßnahmen bei datenverarbeitenden Stellen wurde im September 1979 begonnen. Bis Ende 1986 wurden über 130 Einzelprüfungen durchgeführt. Dabei entfielen 13 % der Kontrollbesuche auf den staatlichen, 74 % auf den kommunalen Bereich und die restlichen 13 % auf den Bereich der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts. Der Prüfungsaufwand vor Ort schlug mit etwa 420 Manntagen zu Buche. Darüber hinaus war für die richtige Einschätzung mancher Einzelprobleme und vor allem für eine praxisorientierte Problemlösung eine Vielzahl von Informationsgesprächen mit Herstellerfirmen von Hard- und Software erforderlich.

Was die Ergebnisse der Prüfungen betrifft, ist festzustellen, daß das Problembewußtsein, Maßnahmen zum Schutz und zur Sicherheit bei der Verarbeitung personenbezogener Daten zu ergreifen, grundsätzlich bei allen betroffenen Stellen vorhanden ist. Diese positive Feststellung gilt nicht nur für den Einsatz der automatisierten Datenverarbeitung, sondern auch für die herkömmliche manuelle Datenverarbeitung.

Der Prüfungsschwerpunkt hat sich in den Bereich der automatisierten Datenverarbeitung verlagert. Um die Risiken beim Einsatz neuer DV-Techniken abschätzen zu können, ist es in verstärktem Maße meinen Mitarbeitern aufgegeben, diese Techniken genau zu analysieren und dann eine praxisbezogene Risikoeinschätzung vorzunehmen, die letztlich zum Einsatz wirkungsvoller Datensicherungsmaßnahmen führen soll. Die genaue Kenntnis neuer DV-Techniken ist die Voraussetzung dafür, wirksame Datensicherungsmaßnahmen vorschlagen zu können.

Prüfungsschwerpunkt ist die **Revisionsfähigkeit** der Datenverarbeitung. Die Revisionsfähigkeit der Datenverarbeitung ist dann beeinträchtigt, wenn, wie bei Prüfungen festgestellt wurde, folgende Mängel anzutreffen sind:

- Fehlen der Programmdokumentation
- Fehlen eines Programmfreigabeverfahrens
- Nichtverwendung von Paßworten und Benutzerberechtigungsprofilen
- Fehlen eines Terminplanes für die Durchführung von Batch-Anwendungen
- Unkontrollierbarer Zugriff von fremdem Personal auf das Rechenzentrum, auf den Rechner oder ganz allgemein auf die gespeicherten Daten
- Ungeregelte Entsorgung von Papierunterlagen
- Unkontrollierbarer Zugang zum Dienstgebäude außerhalb der Dienstzeit.

Es ist äußerst bedenklich, wenn – wie leider immer wieder festzustellen ist – nicht nachweisbar ist, wer wann auf welche Daten zugegriffen hat und wer wann welche Zugriffsberechtigung hatte. Diese zentralen Fragen der Revision müssen aber beantwortbar sein. Andernfalls ist nicht auszuschließen, daß ein Datenmißbrauch unentdeckt bleibt.

Es gibt allerdings auch Datensicherungsprobleme, die der Anwender nur mit Hilfe des Herstellers beheben kann. Gerade für die Revisionsfähigkeit der Datenverarbeitung haben manche Hersteller noch zu wenig getan. Zwar bieten Fremdfirmen für diesen Zweck eine Reihe von Softwareprodukten an. Diese sind allerdings für den Durchschnittsanwender, der kleinere Systeme betreibt, meist nicht einsetzbar, weil diese Software entweder auf diesen Anlagen nicht ablauffähig oder zu aufwendig ist.

Eigentlich möchte man annehmen, daß die Mängel im Laufe der Jahre abnehmen würden. Bei den Kontrollen ist jedoch immer wieder zu bemerken, daß die Datensicherheit für manche datenverarbeitende Stelle Neuland bedeutet. Diese Unkenntnis ist meist darin begründet, daß automatisierte Datenverarbeitung dort erst seit kurzem eingesetzt wird. Die Kontrolle bewirkt eine Verbesserung der Datensicherheit, da man durchwegs bereit ist, die von mir vorgeschlagenen Datensicherungsmaßnahmen einzuführen.

Hingegen gehören beispielsweise Zugangskontrollmaßnahmen und die Verwendung von Paßworten zum Stand der Technik und werden bei allen DV-Installationen durchwegs beachtet.

Die Zeitspanne, die bis zur Behebung der von mir festgestellten Mängel vergeht, ist recht unterschiedlich. Manchmal werden Mängel sehr schnell und, wenn möglich, etwa bei organisatorischen Maßnahmen, sogar noch während der Prüfung behoben. In Einzelfällen kann sich die Mängelbehebung über Jahre hinziehen. Verständnis für lange Bearbeitungszeiten ist wohl dann aufzubringen, wenn

die geplante Maßnahme nur nach Bereitstellung zusätzlicher und verhältnismäßig hoher Haushaltsmittel realisiert werden kann wie etwa bei größeren baulichen Maßnahmen. Solche Situationen entlassen die datenverarbeitende Stelle aber keinesfalls aus ihrer Verantwortung, in der Übergangszeit andere organisatorische Datensicherungsmaßnahmen einzuführen, die das Risiko einer mißbräuchlichen Datenverarbeitung mindern.

Meine Geschäftstelle bietet bereits im Vorfeld der Einführung von DV-Verfahren, bei einer anstehenden Installation einer DV-Anlage oder bei der Planung von Datensicherungsmaßnahmen im Rahmen von Neu- und Umbaumaßnahmen Beratung und Unterstützung an. Dieses Angebot hat große Resonanz gefunden, so daß die Zahl der Beratungen in den letzten Jahren ständig zugenommen hat. In diese Beratungsgespräche fließt häufig eine Vielzahl weiterer Verbesserungsvorschläge ein, die durch die Baumaßnahme selbst nicht veranlaßt sind.

17.3. Sicherungsmaßnahmen bei der Durchführung der Volkszählung 87

Zusätzlich zu den rechtlichen Fragen der Volkszählung (siehe Nr. 11) ergaben sich auch zahlreiche technische und organisatorische Probleme.

17.3.1. Grundsätze

Die Verordnung zur Durchführung der Volkszählung 1987 verlangte von den örtlichen Erhebungsstellen besondere Abschottungsmaßnahmen in organisatorischer, technischer und personeller Hinsicht. Soweit sich die Erhebungsstellen bei der Abwicklung ihrer Aufgaben der maschinellen Datenverarbeitung bedienen, waren besondere technische und organisatorische Maßnahmen vorzusehen, die darauf abstellen, daß eine Verbindung zur Datenverarbeitung des Verwaltungsvollzugs weitgehend unterbunden wird.

Für den Fall, daß die örtliche Erhebungsstelle sich der DV-Einrichtungen der kommunalen Gebietskörperschaft bedient, wurden Datensicherungsmaßnahmen definiert, die als besondere Maßnahmen gelten sollen.

Solche besonderen Maßnahmen sind:

- Innerhalb der Dialoganwendungen muß es gewährleistet sein, daß die Erhebungsstelle nur von ganz bestimmten, vorher festgelegten Bildschirmen der Erhebungsstelle auf den Datenbestand zugreifen kann. Die Verwendung von Benutzerkennungen und Paßworten ist dabei selbstverständlich. Sämtliche Stapelanwendungen werden revisionsfähig innerhalb eigens dafür eingerichteter Prozeduren abgewickelt. Bei Änderung der Prozedur wird eine Versionsnummer mitgeführt, so daß die Entstehungsgeschichte der Prozedur dokumentiert ist. Jeder Verarbeitungslauf wird in einem Ablaufprotokoll maschinell festgehalten, so daß auch hier die Revisionsfähigkeit der Verarbeitung voll gewährleistet ist. Über die Berechtigung auf Daten zuzugreifen, entscheidet ausschließlich die Erhebungsstelle. Das bedeutet, daß die Zugriffsberechtigungen von der Erhebungsstelle definiert und verwaltet werden müssen.
- Magnetbanddateien und Sicherungsbestände sind grundsätzlich in der Erhebungsstelle zu verwahren, es sei denn, die Bestände werden von einem Datenbanksystem verwaltet, so daß die Datenbanksicherung eine Selektierung der einzelnen Bestände vom Sicherungsband aus nicht zuläßt.
- Stapelanwendungen werden grundsätzlich nur dann gestartet, wenn ein schriftlicher Auftrag der Erhebungsstelle vorliegt. Für periodisch wiederkehrende Verarbeitungsläufe existiert ein Terminplan, wobei hier ein Dauerauftrag als ausreichend angesehen wird.
- Werden von Produktionsläufen Druckausgaben angestoßen, so ist bei solchen Fällen immer ein Mitarbeiter der örtlichen Erhebungsstelle im kommunalen Gebietsrechenzentrum anwesend, der die Weiterbehandlung dieser Ausdrucke überwacht. Alle bei diesem Datenverarbeitungsprozeß in der DV-Anlage angelegten Zwischendateien werden nach der Beendigung des Produktionslaufes physikalisch gelöscht.

Diese Maßnahmen wurden von den Erhebungsstellen erfüllt, die sich der automatisierten Datenverarbeitung in einem Mehrzweckrechenzentrum bedienten. Der Einsatz der automatisierten Datenverarbeitung zur Organisation der VZ 87 war allerdings die Ausnahme.

17.3.2. Beratung und Kontrolle der Erhebungsstellen

Die Beratung und Kontrolle der Erhebungsstellen nahm den Hauptanteil der Tätigkeit im ersten Halbjahr 1987 in Anspruch. Bereits in einem frühen Stadium wurden Erhebungsstellen bayerischer Großstädte auf deren Abschottung und technische Sicherung gegen eventuelle Übergriffe von außen untersucht und Ratschläge für die Verbesserung der Sicherungsmaßnahmen gegeben. Auch der DV-Einsatz wurde darauf überprüft, ob die vom Gesetzgeber gebotene Abschottung und Zugriffssicherung bei der maschinellen Verarbeitung in Mehrzweckrechenzentren gegeben sind.

Wie unter 11.1 zum Thema „Volkszählung" bereits erwähnt, wurden vor Beginn der Erhebung bei ca. 100 Erhebungsstellen unterschiedlicher Größenklassen und aus allen Regierungsbezirken die personellen, organisatorischen und technischen Abschottungsmaßnahmen schriftlich abgefragt. Bei den Erhebungsstellen kleinerer Gemeinden lag die Vermutung nahe, daß diese mit der Abschottung Probleme haben könnten, was sich nicht bestätigte. Darüber hinaus wurden ca. 25 Erhebungsstellen besucht, um vor Ort die Wirksamkeit der getroffenen Sicherungsmaßnahmen zu begutachten. Die bei diesen Besuchen vorgefundenen Mängel hielten sich erfreulicherweise in Grenzen, was von dem guten Willen der Verwaltung zeugt, die gesetzlichen Vorgaben ordnungsgemäß zu vollziehen.

Außerdem wurden während der Erhebungsphase mit einer Ausnahme alle Erhebungsstellen der bayerischen Großstädte besucht. Hauptaugenmerk galt dort dem Einsatz der maschinellen Datenverarbeitung. Dabei überraschte, daß der Einsatz von maschineller Datenverarbeitung wesentlich geringer war, als ursprünglich angenommen wurde. Haupteinsatzgebiet der maschinellen Datenverarbeitung war die Verwaltung der Zähler, wobei diese Aufgabe meist auf einem Personal Computer abgewickelt wurde. Nach der Überweisung der Zählerhonorare wurden die Daten auf den maschinell lesbaren Datenträgern gelöscht. Die Abwicklung des Mahnverfahrens wird lediglich in 5 bayerischen Großstädten maschinell unterstützt. Die Prüfung der DV-Verfahren ergab keine Anhaltspunkte, daß Daten über den Rahmen der Zulässigkeit hinaus gespeichert werden.

Die automatisierte Datenverarbeitung für die Volkszählung ist durch technische und organisatorische Maßnahmen von der Datenverarbeitung der übrigen Verwaltung abgeschottet, so daß auch hier kein Grund zu Beanstandungen gegeben war.

Als Schwachstelle bei der Datensicherung erwies sich der in den Durchführungsbestimmungen zur Volkszählung empfohlene Briefkasten bei der Erhebungsstelle, in den Bürger ihre Erhebungsunterlagen selbst einwerfen konnten. Diese Maßnahme, ursprünglich als Bürgerservice gedacht, verleitete in einigen Städten Bayerns Gegner der Volkszählung dazu, in diese Briefkästen Brandsätze und Abfälle zu werfen. In einem Fall wurde der Briefkasten sogar fachmännisch zerlegt und der Inhalt entwendet. Diese Erfahrungen lassen es in der Zukunft angesichts des in der Gesellschaft leider vorhandenen Störpotentials geraten erscheinen, Sicherheitsüberlegungen wieder stärkeres Gewicht beizumessen.

Auch die Entsorgung nicht mehr benötigter VZ-Unterlagen wie Briefumschläge und korrigierte Erhebungsbögen, die neu signiert werden mußten, erfolgte sicher vor Ort in eigenen Papiervernichtungsanlagen.

Der bayerischen Verwaltung ist für die sorgfältige Durchführung der Volkszählung 1987 großes Lob zu zollen.

17.4. Technische Einzelprobleme

Es gibt Probleme technischer und organisatorischer Art, mit denen meine Mitarbeiter immer wieder konfrontiert werden. Es erscheint nur zweckmäßig, über einige Fälle aus der täglichen Arbeit beispielhaft zu berichten.

- Zugangssicherung für ein Rechenzentrum

  Für ein Rechenzentrum, das sensible personenbezogene Daten verarbeitet, habe ich folgende Anforderungen an die Zugangssicherung gestellt:

  Zur Zugangssicherung sind Codekarten zu verwenden, mit denen die Zugangsberechtigung zu verschiedenen Raumzonen innerhalb des DV-Bereiches geregelt werden kann. Die Codekartenleser werden durch Eintasten einer Kennummer zusätzlich gesichert. Der äußere Zugang zum DV-Bereich ist außerdem durch eine Kamera zu überwachen, die auf einem Monitor, der im inneren Sicherheitsbereich installiert ist, anzeigt, wer Einlaß begehrt. Eine solche Maßnahme kommt besonders für die Zeit nach Dienstende, an Wochenenden oder sonstigen dienstfreien Tagen der Sicherheit des Rechenzentrums zugute. Die Kamera ist mit einer Videoaufzeichnung gekoppelt. Für jeden Tag eines Monats steht ein Videoband zur Verfügung, so daß im Bedarfsfall festgestellt werden kann, wer das Rechenzentrum wann betreten hat, weil die Tages- und Uhrzeitangabe eingeblendet werden.

  Schließlich ist es erforderlich, daß für den inneren Sicherheitsbereich ein Abgleich der Zu- und Abgänge (Paarigkeitskontrolle) vorgenommen wird. Damit ist im Notfall feststellbar, wieviele Personen zu welcher Zeit sich im inneren Sicherheitsbereich aufhalten oder aufgehalten haben. Zusätzlich sind unberechtigte Zutrittsversuche festzuhalten. Die Dauer der Speicherung der protokollierten Zugangsdaten, ihre Auswertung und der Umfang ihrer sonstigen Verwendung sollten aber in einer Dienstanweisung – gegebenenfalls nach Absprache mit der Personalvertretung – festgelegt sein.

- Schutz des Rechenzentrums

  An den Schutz eines Rechenzentrums stelle ich folgende Anforderungen:

  Befindet sich ein Rechenzentrum im Erdgeschoß eines Dienstgebäudes, ist eine Außensicherung an den ebenerdigen Fensterfronten unbedingt erforderlich. Das kann beispielsweise durch den Einbau einer durchwurfhemmenden Verglasung, von Glasbruchmeldern mit Anschluß eines Alarmgebers an eine ständig besetzte Leitwarte im Hause u.ä. erreicht werden. Die Installation von Bewegungsmeldern, die Fensterfronten und Zugänge im Innern des DV-Bereiches überwachen, bietet Schutz gegen gewaltsames Eindringen von außen. Der Alarm läuft auch in diesem Falle in der Leitwarte auf.

  Liegt das Rechenzentrum in einem eigenen Brandabschnitt muß darauf geachtet werden, daß keine Sicherheitslücken entstehen. Außerdem muß das Magnetbandarchiv aus dem Rechnerraum entfernt und in einen nahegelegenen möglichst fensterlosen und abgeschlossenen Archivraum verlagert werden. Die Zugangstüre sollte eine Brandschutztüre (Archivtüre) sein, die sich im Brandfall selbsttätig schließt. Sie muß jedoch mit einem Panikschloß ausgestattet sein, so daß sie für den Fall, daß eine Person eingeschlossen worden ist, von innen geöffnet werden kann.

  Damit im Notfall der durch einen Alarm herbeigerufene Sicherheitsdienst rechenzentrumsfremde Personen erkennen kann, sollten alle im Rechenzentrum beschäftigten Personen zu ihrer Identifizierung sichtbar Lichtbildausweise tragen. Sie können mit den Funktionen der Codekarte zur Zugangskontrolle kombiniert werden.

  Auch für dezentrale Systeme, die rund um die Uhr betriebs- und auskunftbereit sein müssen, sind entsprechende Sicherungsmaßnahmen zu treffen, sofern diese Systeme in ebenerdigen Räumen installiert sind.

- Programmentwicklung

  Es gibt Installationen, bei denen der DV-Hersteller auch für die Entwicklung und Wartung der Anwendungsprogramme verantwortlich ist. Grundsätzlich sollte dabei mit Testdaten gearbeitet werden. Für den Abschlußtest und im Rahmen der Wartung ist die Weitergabe von personenbezogenen Daten nicht auszuschließen. Gleiches gilt für die Reparatur defekter Datenträger durch die Herstellerfirma in deren Werk. In solchen Fällen sind vertragliche Zusatzvereinbarungen im Rahmen der Wartung zu treffen, deren Ziel es ist, die Sicherheit und Geheimhaltung der Daten zu gewährleisten. Da in erster Linie die speichernde Stelle für die Maßnahmen zum Datenschutz und zur Datensicherung die Verantwortung trägt, ist hier eine sorgfältige Prüfung dieser Maßnahmen erforderlich.

- Entsorgung von Datenträgern

  Bei der Vernichtung von Datenträgern sind die Festlegungen der deutschen Sicherheitsnorm DIN 32757 Teil I und Teil II, die im Oktober 1985 verabschiedet wurden, heranzuziehen. In dieser Norm sind für die Vernichtung 5 Sicherheitsstufen definiert, wobei die

Stufe 1 die geringste und die Stufe 5 die höchste Sicherheit bedeutet. Die Vernichtung von Unterlagen mit personenbezogenen Daten ist in der Regel der Sicherheitsstufe 3 zuzuordnen. Nach DIN 32757 gelten in der Sicherheitsstufe 3 für die Vernichtung von Papier folgende Grenzwerte:

- Streifen mit einer Schnittbreite kleiner/gleich 2 mm und einer Schnittlänge bis unendlich oder
- Partikel bis zu einer Größe von 240 qmm.

Ab der Sicherheitsstufe 4 gilt Papier erst dann als vernichtet, wenn die Materialteilchenbreite (Partikel) kleiner/gleich 2 mm und die Materialteilchenlänge kleiner/gleich 15 mm ist.

Bei der Vernichtung von Mikrofilmen darf die Partikelgröße nur 1 qmm betragen.

- Aufbewahrung von sensiblen Unterlagen

Unterlagen mit sensiblen personenbezogenen Daten, z.B. mit medizinischen Daten, müssen gegen eine Kenntnisnahme durch unbefugte Dritte gesichert sein. Möglichkeiten, die unbefugte Kenntnisnahme durch Dritte zu verhindern, sind unter anderem das Abschließen der Räumlichkeiten, die Bereitstellung verschließbarer Behältnisse, und der Erlaß entsprechender Dienstanweisungen. In Bearbeitung befindliche Vorgänge müssen nach Dienstsschluß weggesperrt werden und dürfen nicht auf den Schreibtischen verbleiben. Der für die Einhaltung des Datenschutzes zuständige Bedienstete einer Behörde hat sich deshalb durch gelegentliche Kontrollen davon zu überzeugen, ob die getroffenen Anordnungen auch eingehalten werden.

- Dienstanweisung für den Betrieb einer dezentralen DV-Anlage

Es ist sehr zu begrüßen, wenn eine öffentliche Stelle, die im Zuge der Dezentralisierung der Datenverarbeitung eine eigene DV-Anlage erhält, den ordnungsgemäßen Betrieb dieser DV-Anlage in einer Dienstanweisung regelt.

Es ist aber nicht einfach, schon zu Beginn für alle Probleme, die bei der maschinellen Datenverarbeitung auftreten können, wirksame Lösungen zu haben. Oft stellt sich die Brauchbarkeit mancher Sicherungsmaßnahmen erst im laufenden Betrieb heraus. Deshalb ist es durchaus sinnvoll, sich in manchen Bereichen zunächst nur auf Verbote oder vorläufige Anordnungen zu beschränken, bis praktikable Lösungen erkannt worden sind.

In einer Dienstanweisung für den Betrieb dieser DV-Anlagen sollen u.a. auch Regelungen über die Wartung der Festplattenspeicher, über die Modalitäten der Auslagerung der Sicherheitskopien, Maßnahmen zur Vernichtung von magnetischen Datenträgern, Vorschriften über den Transport der Datenträger, Regelungen über die Vergabe von Zugriffsberechtigungen bei Vertretungen infolge von Krankheit und Urlaub sowie Regelungen zur Überprüfung der Einhaltung der durch die Dienstanweisung vorgegebenen Maßnahmen enthalten sein.

17.5. Orientierungshilfen zur Datensicherung

Neben den Tätigkeitsberichten, die eine Informationsquelle für die datenverarbeitenden Stellen darstellen, wurden in der Vergangenheit in meiner Dienststelle eine Reihe von Orientierungshilfen für Datensicherungsmaßnahmen erstellt. Die wichtigsten seien an dieser Stelle erwähnt.

Aufbauend auf dem Schutzstufenkonzept, das von einer Arbeitsgruppe des staatlichen Koordinierungsausschusses Datenverarbeitung entwickelt wurde, wurden Orientierungshilfen für Datensicherungsmaßnahmen beim Einsatz dezentraler Datenverarbeitungsanlagen und bei manueller Datenverarbeitung erstellt. Diese Orientierungshilfen fanden regen Anklang und enthalten abhängig von der Sensitivität der zur verarbeitenden Daten, Vorschläge für Datensicherungsmaßnahmen.

Außerdem wurden Orientierungshilfen zu speziellen technischen Fragen erstellt.

Wegen der Dezentralisierung der Datenverarbeitung und vor allem aus Kostengesichtspunkten gewann die von den Herstellern angebotene Fernwartung der DV-Systeme immer mehr an Bedeutung. Aus diesem Grunde wurden die Fernwartungskonzepte der wichtigsten Hersteller untersucht und Anregungen für einzuführende Sicherungsmaßnahmen beim Einsatz der Fernwartung gegeben. Diese Orientierungshilfen werden dem Stand der Technik angepaßt und fortgeschrieben.

Für die Revision ist das Nachvollziehen der maschinellen Datenverarbeitung eines der wichtigsten Themen. Aus diesem Grunde wurde ein Anforderungskatalog für die Aufzeichnung und maschinelle Auswertung von Ablaufdaten erstellt und eine Bestandsaufnahme für die wichtigsten, im öffentlichen Bereich eingesetzten, Betriebssysteme durchgeführt.

Mit zunehmendem Einsatz der Personal Computer gewinnt das Thema „Datensicherung in der Individuellen Datenverarbeitung" an Bedeutung. Im 8. Tätigkeitsbericht wurde in der Anlage 3 eine Orientierungshilfe für Datensicherungsmaßnahmen beim Einsatz von Personal Computern gegeben.

Schließlich haben Mitarbeiter meiner Geschäftsstelle Ende 1986 ein fast 500 Seiten umfassendes Kompendium über die Datensicherung vorgelegt, das über den Buchhandel zu beziehen ist und in dem alle modernen Informationstechniken, deren Einsatzmöglichkeiten und deren Risiken sowie geeignete Sicherheitsmaßnahmen ausführlich behandelt werden. (Abel/Schmölz, Datensicherung für Betriebe und Verwaltung).

18. Datenschutzregister

Nach § 7 der Verordnung über das Datenschutzregister (DSRegV) vom 23.11.1978 haben die speichernden Stellen (Art. 5 Abs. 3 Nr. 1 Bayer. Datenschutzgesetz) über die obersten Dienstbehörden die registerpflichtigen Angaben über die Verarbeitung personenbezogener Daten in automatisierten Verfahren dem Landesbeauftragten für den Datenschutz zu melden.

Die nachstehende Tabelle soll die Entwicklung des Datenschutzregisters, dessen Veröffentlichung gesetzlich

vorgeschrieben ist (§ 8 DSRegV), zu den Stichtagen veranschaulichen.

Zeitpunkt	speichernde Stellen	Dateien
01.01.1980	2537	8336
01.11.1980	3057	10126
15.10.1981	3383	11318
01.10.1982	3676	12341
01.11.1983	3873	13095
20.11.1984	4127	14228
28.11.1985	4343	15285
26.11.1986	4577	15999

Im Jahre 1986 fiel die absolute Zahl der Zunahmen bei den Dateimeldungen auf 711, das sind 340 weniger als im Vorjahr. Hingegen stieg die Zahl der speichernden Stellen um 235. Die Anzahl der Dateien unterschiedlichen Aufbaus beträgt nach dem Stand vom 26.11.1986 2.285. Diese geringe Zahl erklärt sich daraus, daß sich viele speichernde Stellen sogenannten Gemeinschaftsverfahren angeschlossen haben. So enthält das Datenschutzregister beispielsweise 2 500 Dateien, die für die Besoldung der Bediensteten der speichernden Stellen geführt werden. Diese 2500 Dateien werden in lediglich 121 unterschiedlichen Verfahren verarbeitet. Ähnlich ist die Situation im automatisierten Einwohnerwesen. Hier wurden von den Gemeinden 1119 automatisierte Einwohnerdateien gemeldet, die nach 113 unterschiedlichen Verfahren betrieben werden.

Die Meldungen zum Datenschutzregister werden manuell verwaltet. Zur Erstellung der Übersicht und zur Auskunft an den Betroffenen sind auf einem Textsystem Name und Anschrift der speichernden Stelle und die Bezeichnung der Datei gespeichert. Auf diese Weise kann ich, wie bereits in früheren Tätigkeitsberichten mitgeteilt, Petenten eine auf seinen Wohnort bezogene Liste aller in Frage kommenden speichernden Stellen und der dort geführten Dateien übersenden. Gegenüber 1985 stieg die Anzahl dieser Auskünfte aus dem Datenschutzregister um ca. 160 auf 270.

Um Anhaltspunkte für die Pflege des Datenschutzregisters zu erhalten, werden Daten protokolliert, die eine Arbeitsanfallstatistik zulassen. Für den Zeitraum vom 21.7.1986 bis 11.12.1986 ergaben sich beispielsweise folgende Zahlen (für den gesamten Berichtszeitraum liegen keine genauen Zahlen vor, da das DV-Verfahren erst Mitte 1986 zum Einsatz kam):

Neueintragen einer speichernden Stelle:	198
Neueintragen einer Datei bei einer speichernden Stelle:	755
Datenänderung bei einer speichernden Stelle:	42
dateibezogene Datenänderung:	36
Löschen einer speichernden Stelle:	23
Löschen einer Datei:	177

Änderungen im Datenschutzregister werden jährlich in einem Nachtrag im Staatsanzeiger veröffentlicht. Derartige Veröffentlichungen von Nachträgen sind für die Bürger wenig aufschlußreich. Der Vorsitzende des Beirats beim Landesbeauftragten für den Datenschutz hat deshalb vorgeschlagen, auf die Veröffentlichung des jährlichen Nachtrags zu verzichten. Dieser Vorschlag wird gegenwärtig geprüft.

19. Datenschutz beim Bayerischen Rundfunk

Nach Art. 21 Abs. 3 BayDSG wird die Einhaltung des Datenschutzes im Bayerischen Rundfunk vom dortigen Datenschutzbeauftragten überwacht, der jährlich über seine Tätigkeit einen Bericht erstattet. Diesen Bericht hat er auch dem Landesbeauftragten für den Datenschutz zu übermitteln (Art. 21 Abs. 3 Satz 6 BayDSG). Hieraus leite ich wie schon in den Jahren zuvor für mich die Aufgabe ab, kurz über den Datenschutz beim Bayer. Rundfunk zu berichten. Dem Bericht des Datenschutzbeauftragten des Bayerischen Rundfunks für den Zeitraum vom 1.1. bis 31.12.86 lassen sich folgende Schwerpunkte entnehmen:

Bei der Überwachung der Datenverarbeitung beim Bayerischen Rundfunk (BR) hat der Datenschutzbeauftragte wiederum keine Datenschutzverstöße festgestellt. Im Mittelpunkt standen wie auch im letzten Jahr der Personal- und der Programmbereich.

Personalbereich:

- Hier befaßt sich der Bericht mit der Zulässigkeit der Weitergabe von sogenannten Vergleichsmitteilungen, mit denen die einzelnen „Arbeitgeber" des öffentlichen Dienstes gezahlte Vergütungen (z. B. Kindergeldzuschlag) untereinander vergleichen. Nicht nur die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten, sondern auch andere dafür zuständige Behörden des Bundes und der Länder forderten von den Rundfunkanstalten die Beteiligung an diesem Verfahren. Hierfür fehle eine Rechtsgrundlage. Die anfordernden Behörden (regelmäßig die Besoldungsstellen) müßten daher künftig die gewünschten Auskünfte unmittelbar von ihren Bediensteten erfragen.

- Bei der Telefondatenerfassung sei auch unter Berücksichtigung der Entscheidung des Bundesarbeitsgerichts vom 27.5.1986 – 1 ABR 48/84 – eine materielle Änderung der beim BR geltenden Regelung nicht erforderlich. Mittlerweile sei anerkannt, daß die Telefondatenerfassung bei Dienstgesprächen datenschutzrechtlich zulässig sei. Dies müsse erst recht gelten, wenn beim BR nunmehr die Telefonnummer des Angerufenen in jedem Fall anonymisiert werde. Bei Privatgesprächen sei es notwendig, die Mitarbeiter in umfangreicher Weise über die Zulässigkeit der Gespräche und über den Umgang mit den entstandenen Daten aufzuklären. Hinweise des Hauses seien hierzu noch nicht erlassen.

- Der Rundfunkdatenschutzbeauftragte vertritt die Auffassung, daß dem Personalrat Unterlagen mit personenbezogenen Mitarbeiterdaten grundsätzlich nur mit schriftlicher Zustimmung der Mitarbeiter überlassen werden dürften. Ansonsten sei nur eine mündliche Information zulässig.

- Wie auch schon im Vorjahr setzt sich der Bericht mit den Kontrollmitteilungen der Rundfunkanstalten an die Finanzbehörden über Honorarzahlungen an im Ausland ansässige Steuerpflichtige auseinander. Mittlerweile hat das Bundesamt für Finanzen allerdings klargestellt, daß die Informationsklauseln in den einzelnen Doppelbesteuerungsabkommen ausreichende Rechtsgrundlagen für die Kontrollmitteilungen darstellten. Fehlten solche Doppelbesteuerungsabkommen, würden entsprechende

Mitteilungen nicht gemacht. Der Datenschutzbeauftragte hat nun seine früheren Bedenken zurückgestellt.

Programmbereich:

- Im Programmbereich schildert der Datenschutzbeauftragte seine Rechtsauffassung zur Kennzeichnung von Musiktiteln in der zentralen Schallplattenkatalogisierung im Deutschen Rundfunkarchiv, an denen Rundfunkmitarbeiter urheberrechtlich beteiligt sind. Im Ergebnis hält er eine Übermittlung der Namens- und Pseudonymliste der Rundfunkanstalten an das Deutsche Rundfunkarchiv für zulässig. Um den Eingriff in die Rechte der Betroffenen möglichst gering zu halten, soll in den Schallplattenkatalog aber nur ein abstrakter Hinweis über die urheberrechtliche Beteiligung festangestellter Rundfunkmitarbeiter an einem bestimmten Musiktitel aufgenommen werden.

- Auf Anfrage des Bayerischen Landesbeauftragten für den Datenschutz habe sich der Rundfunkdatenschutzbeauftragte mit der weiteren Verwendung der an die Serviceredaktion übermittelten Fahndungsersuchen der Polizei befaßt. Die Fahndungsersuchen und die hieraus redaktionell erstellten Fahndungsmeldungen würden bis zum Jahresende in der Redaktion und anschließend in der Registratur für weitere zwei Jahre besonders verwahrt. Anschließend würden sie in einem kontrollierten Verfahren vernichtet.

Wie in den Vorjahren nimmt der Themenbereich Gebühreneinzug (Datenschutz bei der GEZ) auch im Berichtsjahr einen breiten Raum im Tätigkeitsbericht des Rundfunkdatenschutzbeauftragten ein.

- Der Umfang von Anfragen an die GEZ mit datenschutzrechtlichem Bezug sei im Berichtsjahr erneut deutlich zurückgegangen. Der interne Datenschutzbeauftragte der GEZ habe im Jahr 1986 nur 28 Anfragen bearbeitet. Dies müsse in Relation dazu gesehen werden, daß bei der GEZ zum 31.12.1986 insgesamt 25.916.013 Hörfunkteilnehmer und 23.020.526 Fernsehteilnehmer gemeldet seien.

- Die Direktwerbemaßnahmen der GEZ waren erneut Gegenstand von Beratungen der Rundfunkdatenschutzbeauftragten. Nunmehr sollen erstmals von einem Direktwerbeunternehmen erworbene Adressen von Gewerbetreibenden und Firmen mit dem bestehenden GEZ-Datenbestand abgeglichen und angeschrieben werden, um eine besonders große Zahl von Anmeldungen von Rundfunkgeräten zu erreichen.

- Die Aktualisierung der Lastschriftzahleradressen bereite weiterhin Probleme. Die hierüber mit dem Kreditgewerbe geführten Verhandlungen hätten noch zu keinem zufriedenstellenden Abschluß geführt. Insbesondere sähen sich die Spitzenverbände des Kreditgewerbes auf Grund des Bankgeheimnisses nicht in der Lage, das ursprüngliche Verfahren der Meldung aller Anschriftenänderungen wieder aufzunehmen.

- Die Probleme, ob und in welchem Umfang die Beauftragten der Rundfunkanstalten Einzelauskünfte von Meldebehörden und Kraftfahrzeugzulassungsstellen erhalten könnten, würden in Zusammenarbeit mit den beteiligten Ressorts zufriedenstellend gelöst.

Neben den Problemen der Teilnehmerdatenkarten, die die Beauftragten der Rundfunkanstalten als wichtiges Arbeitsmittel benötigten und den Fragen des Datenschutzes in der Rundfunkgebührenstelle, die es erlaube, Daten des GEZ-Bestandes automatisch in Briefe einzufügen, hatte sich der Rundfunkdatenschutzbeauftragte mit einer Vielzahl weiterer datenschutzrechtlich relevanter Einzelfälle zu befassen.

Zusammenfassend stellt der Datenschutzbeauftragte des Bayerischen Rundfunks fest, daß die Rundfunkteilnehmer offensichtlich kaum mehr Zweifel an der Einhaltung des Datenschutzes beim Rundfunkgebühreneinzug hätten. Dies zeige der weitere Rückgang der Zahl der Auskunftsersuchen und der sonstigen Anfragen von Rundfunkteilnehmern und Dritten in bezug auf den Datenschutz im Vergleich zu den Vorjahren. Bei den Anfragen stehe in aller Regel nicht die datenschutzrechtliche Problematik im Vordergrund. Die Rundfunkteilnehmer versuchten statt dessen regelmäßig, auf diesem Wege eine angeblich unzutreffende Sachbearbeitung beim normalen Gebühreneinzug noch zu korrigieren. Die bei der GEZ getroffenen Datenschutz- und Datensicherungsmaßnahmen seien wirksam und voll ausreichend. Trotzdem sei die GEZ jetzt und in Zukunft um weitere Verbesserung auf diesem Gebiet bemüht.

20. 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. Die Landtagswahl führte daher zu einer Neubestellung der meisten Mitglieder des Beirats. Dem neuen Beirat gehören nun an:

Ordentliche Mitglieder	Vertreter
Die Landtagsabgeordneten	
Franz Brosch	Willi Baumann
Adolf Dinglreiter	Franz Xaver Werkstetter
Dieter Heckel	Anneliese Fischer
Peter Welnhofer	Adolf Beck
Klaus Warnecke	Armin Nentwig
Carmen König	Hedda Jungfer
Die Senatoren	
Wolfgang Burnhauser	Hartwig Reimann
Für die Staatsregierung	
Dr. Klaus Geiger Ministerialdirigent im Bayerischen Staatsministerium der Finanzen	Joachim Schweinoch Ministerialdirigent im Bayerischen Staatsministerium des Innern
Für die Kommunalen Spitzenverbände	
Dr. Georg Wilhelm Geschäftsleitender Direktor der Anstalt für Kommunale Datenverarbeitung in Bayern	Klaus Eichhorn Direktor der Anstalt für Kommunale Datenverarbei tung in Bayern
Für die Sozialversicherungsträger	
Franz Martin Fehn Erster Direktor der Landes-	Herbert Schmaus Verwaltungsdirektor beim

versicherungsanstalt Oberfranken und Mittelfranken	AOK-Landesverband Bayern

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

Dr. med. Hans Braun Präsident des Verbandes der Freien Berufe Bayern e. V.	Winfried Wachter Präsidiumsmitglied des Verbandes Freier Berufe in Bayern e. V.

In seiner konstituierenden Sitzung am 27.1.1987, die gleichzeitig die 32. Sitzung des Beirats war, wählte der Beirat aus seinen Reihen

MdL Franz Brosch zum Vorsitzenden und
MdL Klaus Warnecke zum Stellvertreter des Vorsitzenden.

Der Beirat befaßte sich in den beiden Sitzungen am 27.1.1987 und 24.3.1987 mit folgenden Themen:

- Beratung des 8. Tätigkeitsberichts und der inzwischen veranlaßten Maßnahmen;
- Eingaben aus dem Bereich der Justiz, Frage der Kontrollkompetenz des Datenschutzbeauftragten;
- Sachstandsbericht zum Datenschutz bei der Volkszählung;
- Übermittlung von Wähleranschriften an politische Parteien und Wählergruppen (Art. 35 Abs. 1 MeldeG);
- Zulässigkeit von Auskünften der Krankenhäuser über die für den Tod ursächlichen Krankheiten und Umstände an Angehörige der Verstorbenen;
- Stand der Dienstanweisungen zum Verfassungsschutz;
- Beanstandungen nach Art. 30 Abs. 1, 29 Abs. 5 Satz 2 BayDSG.

In der 34. Beiratssitzung am 14. Juli 1987 verabschiedete sich der bisherige Datenschutzbeauftragte Dr. Stollreither mit einem Überblick über Erfahrungen aus neun Jahren Datenschutz von den Beiratsmitgliedern.

21. Behandlung des 8. Tätigkeitsberichtes im Parlament

Der 8. Tätigkeitsbericht wurde am 27. Januar 1987 im Ausschuß für Verfassungs-, Rechts- und Kommunalfragen des Bayerischen Landtags und am 11. Februar 1987 im Rechts- und Verfassungsausschuß des Bayerischen Senats beraten.

1. Bei der Beratung im Bayerischen Landtag wies der Berichterstatter, Abgeordneter Franz Brosch, auf die datenschutzrechtlich positive Entwicklung im Bereich des Gesundheitsdienstes und des Krankenhausgesetzes hin. Er bestätigte die Bedeutung des Datenschutzes im Polizeibereich und hob Verbesserungen des Datenschutzes bei Polizeipräsidien sowie beim Polizeipräsidium München, bei dem aufgrund der Datenschutzkontrollen problematische Datenspeicherungen entschärft wurden, hervor. Im Einzelfall müßten erkannte systematische und individuelle Fehler bekämpft werden. Das Innenministerium bemühe sich um rasche Abhilfe. Zur unzulässigen Verwendung von Steuerdaten für andere Zwecke der Gemeinden wünschte sich der Berichterstatter eine Änderung der Abgabenordnung. Befriedigt äußerte er sich darüber, daß die Volkszählung keine grundsätzlichen datenschutzrechtlichen Bedenken auslöse. Hinsichtlich des technischen und organisatorischen Datenschutzes hielt der Berichterstatter die beratende Tätigkeit des Datenschutzbeauftragten gegenüber der Verwaltung für sehr hilfreich. Schnelle Verknüpfbarkeit und Verfügbarkeit von Daten sowie große Speicherfähigkeit der Dateien seien notwendig. Sie müßten aber der Kontrolle des Datenschutzbeauftragten unterliegen. Nicht jede einzelne Akte bedürfe jedoch dafür der Regelung durch das Bundesdatenschutzgesetz; diese Regelungsfrage stelle sich den Ländern.

Mitberichterstatter MdL Warnecke hob hervor, daß kein einziger Fall in Bayern bekannt sei, in dem die Aufklärung eines Verbrechens oder eine Fahndungsmaßnahme durch den Datenschutz behindert worden sei. Er betonte die Notwendigkeit gesetzlicher Ermächtigungen für die Speicherung personenbezogener Daten. Hinsichtlich der beanstandeten Datenspeicherungen beim Polizeipräsidium München vertrat er die Ansicht, daß hier nicht persönliche Fehler kleiner Beamter, sondern ein systematischer Defekt vorgelegen habe. Er wies besonders auf die Probleme beim Datenschutz zwischen Vormundschaftsgerichten, Führerscheinstellen und Psychiatrie hin. Ein auf Dauer psychisch Behinderter oder Kranker könne in der Tat kein Fahrzeug führen. Dies gelte jedoch nicht für nur zeitweise in ihren Fähigkeiten eingeschränkte Menschen, die im Straßenverkehr nicht krankheitsbedingt gefährlicher seien als die an anderen nicht erfaßten Krankheiten leidenden Bürger. Wichtig sei die Anmerkung des Datenschutzbeauftragten, daß Arztberichte und Rechnungen direkt an Betriebskrankenkassen, nicht jedoch an den Betrieb selbst übersandt werden dürften. Zum Bereich Justiz erinnerte der Mitberichterstatter an die Notwendigkeit einer gesetzlichen Regelung der Übermittlung gerichtlicher Entscheidungen an staatliche und nichtstaatliche Stellen. Im technischen und organisatorischen Datenschutzbereich nahm sich der Mitberichterstatter vor allem des Themas Bürokommunikation an. Er hielt die Datenschutzkontrolle bei kleinen und kleinsten Einheiten für besonders schwierig.

In der Aussprache nahm sich MdL Bäumer besonders Datenschutzfragen im Bereich von Sicherheitsbehörden an und verwies auf einschlägige Passagen der Begründung des Volkszählungsurteils des Bundesverfassungsgerichts. Er meinte, solange Bürger in der Ausübung ihrer verfassungsmäßigen Rechte – Meinungs- und Demonstrationsfreiheit – gespeichert würden, sei den Ausführungen des Bundesverfassungsgerichts nicht Rechnung getragen. Zur Volkszählung bezweifelte er, daß in kleinen Gemeinden die geforderte Abschottung gewährleistet sei.

MdL Professor Dr. Maier klagte über Schwierigkeiten für Wissenschaftler, in Archiven an personenbezogene Daten heranzukommen. Unter Beachtung der Datenschutzvorschriften müßten Archive für Wissenschaft und Forschung zugänglich sein.

2. Der Rechts- und Verfassungsausschuß des Bayerischen Senats griff bei der Erörterung des Tätigkeitsberichts eine Reihe wichtiger Fragen auf:

   Senator Dr. Schumann erkundigte sich nach dem Fortschritt des Archivgesetzes, machte auf die Problematik aufmerksam, die sich aus der Telekommunikationsordnung ergebe, und fragte nach dem Vollzug des Senatsbeschlusses vom Februar 1985 zur Angabe der Auswirkungen von Gesetzesvorhaben auf personenbezogene Daten. Senator Dr. Wrede sprach Probleme des Bildschirmtextes an. Senator Dr. Arneth erkundigte sich nach Datenschutzfragen im Zusammenhang mit dem Personalausweisgesetz der Staatsregierung. Senator Dr. Wrede warf die Frage „Meldepflicht bei AIDS" auf. Senator Gebhard betonte die wichtige Rolle des Datenschutzes im Beihilfeverfahren. Senator Thallmair erkundigte sich nach der Möglichkeit, Daten über einen Bauantrag in öffentlicher Gemeinderatssitzung bekanntzugeben. Senator Dr. Merk fragte, ob es datenschutzrechtlich unbedenklich sei, wenn ohne Zustimmung eines Patienten von Seiten des Arztes eine Abrechnungstelle eingeschaltet werde, die dabei Daten erhalte. Er erkundigte sich weiter nach den Möglichkeiten des Dienstherrn, mißbräuchliche Nutzungen des Diensttelefons, die zu beachtlichen Kosten führen könne, zu kontrollieren. Der Landesbeauftragte für den Datenschutz und der Vertreter des Bayerischen Staatsministeriums des Innern nahm zu diesen Fragen jeweils Stellung.

22. Konferenz der Datenschutzbeauftragten

Die Datenschutzbeauftragten der Länder und des Bundes und die Datenschutzkommission Rheinland-Pfalz haben im Berichtszeitraum auf vier Tagungen gemeinsam interessierende Fragen erörtert. Beispielhaft seien genannt eine Aussprache über den Stand datenschutzrelevanter Gesetzgebungsvorhaben, Datenschutzfragen im Zusammenhang mit der Novellierung der Strafprozeßordnung, des Ausländerzentralregisters, der Statistik und technisch-organisatorische Datenschutzfragen. Sie befaßten sich mit der Volkszählung 1987, mit Fragen der Datenverarbeitung der Kriminologischen Zentralstelle in Wiesbaden. Längere Erörterungen wurden der Bewertung von Datenschutzvorkehrungen für die Volkszählung gewidmet. Die Datenschutzbeauftragten befaßten sich außerdem mit dem Entwurf einer Fahrzeugregisterverordnung und tauschten in einer größeren Zahl von Einzelfragen Erfahrungen aus. Die gemeinsame Erörterung von Datenschutzfragen aus dem Bereich der Gentechnologie und der Datenverarbeitung im Zusammenhang mit AIDS wurde beschlossen. Gegenstand der vierten Sitzung war die Zulässigkeit der Speicherung von HIV-Infektionen im polizeilichen Informationssystem. Zu dieser Frage konnte keine gemeinsame Haltung gefunden werden. Der Vorschlag der Mehrheit der Datenschutzbeauftragten konnte von mir wegen zahlreicher Widersprüche und offener Unklarheiten nicht mitgetragen werden. Ich habe deshalb meine Auffassung zu diesem Thema dem Vorsitzenden der Innenministerkonferenz mitgeteilt. Meine Auffassung ist in 4.5.3 niedergelegt.