

Der Landesbeauftragte für den Datenschutz
Nr. DSB/1 - 510 - 4

München, den 26. Mai 1981

An den
Herrn Präsidenten
des Bayerischen Landtags
München

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

Sehr geehrter Herr Landtagspräsident!

Anliegend übersende ich gemäß Art. 28 Abs. 4 des Bayerischen Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 den dritten Tätigkeitsbericht für den Zeitraum vom 1. Januar bis 31. Dezember 1980.

Der Beirat hat den Entwurf in seiner Sitzung am 19. Mai 1981 vorberaten.

Mit vorzüglicher Hochachtung

Dr. Stollreither

Dritter Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

mit Schreiben vom 26. Mai 1981 dem Bayerischen Landtag und der Bayerischen Staatsregierung gemäß Art. 28 Abs. 4 des Bayerischen Datenschutzgesetzes erstattet.

Berichtszeitraum: 1. Januar bis 31. Dezember 1980

Inhaltsübersicht

	Seite
1. Vorbemerkung	3
1.1 Übersicht	3
1.2 Zur Lage	3
1.2.1 Beirat	4
1.2.2 Personal der Geschäftsstelle	4
1.2.3 Datenschutzregister	4
1.2.4 Konferenzen der Datenschutzbeauftragten	5
1.2.5 Anrufung des Landesbeauftragten für den Datenschutz, Auskunft „über die gespeicherten Daten“	5
2. Grundsätzliche Fragen und neue Probleme	5
2.1 Fortentwicklung des Datenschutzrechts	5
2.2 Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz	7
2.3 Erhebung von Daten	7
2.4 Besondere datenschutzrechtliche Freigabe von neuen Verfahren der automatischen Datenverarbeitung	8
2.5 Datenverarbeitung im Auftrag	8
2.6 Neue Medien – Überblick	9
2.7 Technische Zukunftsfragen	9
3. Einzelfragen	10
3.1 Melde- und Standesamtswesen	10
3.1.1 Meldescheine	10
3.1.2 Übermittlung von Anschriften aus dem Melderegister an Parteien	10
3.1.3 Gruppenauskunft aus dem Melderegister an Verbände und Vereine	10
3.1.4 Weitergabe und Veröffentlichung von Angaben durch das Standesamt	10
3.2 Sicherheitsbereich	11
3.2.1 Rasterfahndung durch die Polizei	11
3.2.2 Kriminalpolizeiliche Sammlungen (KPS)	12
3.2.3 Sperrung von Daten bei der Polizei	12
3.2.4 Löschung von Daten bei der Polizei	13

	Seite		Seite	
3.2.5	Datenübermittlung durch die Polizei	13	3.6.3 Erhebung von Namen und Anschriften der Betroffenen für die Sozialhilfestatistik	22
3.2.6	Registrierung von Reisenden an der Grenze	13	3.6.4 Schülerbefragung im Absolventenjahrgang der Sekundarstufe II (Abiturientenbefragung)	22
3.2.7	Datenabgleich zwischen Kraftfahrzeug-Zulassungsstellen und der Polizei	14	3.7 Personalwesen	23
3.2.8	Datenerhebung durch Abschleppunternehmen im Auftrag der Polizei	14	3.7.1 Zulässigkeit der Registrierung dienstlicher Telefongespräche	23
3.2.9	Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen	14	3.7.2 Weitergabe der Anschriften von Bewerbern für die Beamtenlaufbahn an Versicherungen	23
3.2.10	Gutachtenverwaltung im Bayer. Landeskriminalamt	15	3.7.3 Personalnachrichten der staatlichen Bibliotheken	24
3.2.11	Verfassungsschutz	15	3.7.4 Aufbewahrung von Gleitzeit-Erfassungskarten	24
3.2.11.1	Ergebnis bisheriger Überprüfungen	15	3.7.5 Veröffentlichung von Angaben über Behördenpersonal in Adreßbüchern	24
3.2.11.2	Mitteilungen über das Prüfungsergebnis	15	3.8 Berührungspunkte mit öffentlich-rechtlichen Religionsgesellschaften	24
3.2.11.3	Weitergabe von Daten des Verfassungsschutzes an ausländische Geheimdienste	16	3.9 Neue Medien	25
3.3	Justiz	16	3.9.1 Anwendungen	25
3.3.1	Mitteilung in Strafsachen (MiStra)	16	3.9.2 Pilotprojekt	25
3.3.2	Zentraldateien der Staatsanwaltschaften	17	3.9.3 Datenschutzrechtliche Probleme	26
3.3.3	Prozeßkostenhilfe	17	3.9.4 Grundsätze für den Datenschutz	26
3.3.4	Benachrichtigung des Finanzamts über die Entschädigung für Strafverfolgungsmaßnahmen	17	3.9.5 Erforderlichkeit eines Gesetzes?	28
3.3.5	Schuldnerverzeichnis	18	3.10 Verschiedenes	28
3.4	Sozial- und Gesundheitsbereich	18	3.10.1 Lichtbilder	28
3.4.1	Besondere Vorschriften über den Datenschutz im 10. Buch des Sozialgesetzbuches (SGB X)	18	3.10.2 Öffentliche Zustellungen aufgrund des Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetzes	28
3.4.2	Einsichtnahme in Sozialhilfeunterlagen durch Mitarbeiter einer Hochschule	19	3.10.3 Datengeheimnis – sonstige Nutzung von Daten	29
3.4.3	Anwendbarkeit des Bundesdatenschutzgesetzes auf Krankenhäuser	20	3.10.4 Auskunftsverweigerung „aus Gründen des Datenschutzes“	29
3.4.4	Übermittlung von Patientendaten durch Krankenhäuser zu Werbezwecken	20	3.10.5 Tätigkeit von Kommunalbediensteten für Kreditauskunfteien	29
3.5	Schul- und Hochschulbereich	20	3.11 Allgemeine Feststellungen zur Kontrolltätigkeit im Bereich der technischen und organisatorischen Maßnahmen (Art. 15 BayDSG)	29
3.5.1	Verwendung von Gesundheitskarten bzw. Gesundheitsbogen an Schulen	20	3.11.1 Prüfung der technischen und organisatorischen Datensicherungsmaßnahmen in Rechenzentren	30
3.5.2	Weitergabe von Schülerdaten an Kreditinstitute	21	3.11.2 Datensicherungsmaßnahmen bei Universitätskliniken	30
3.5.3	Bezeichnung „Sonderschule“ auf Schülerausweisen	21	3.11.3 Prüfung der technischen und organisatorischen Sicherungsmaßnahmen bei Kommunalbehörden	31
3.5.4	Datenerhebung für Kindergärten	21	3.11.4 Prüfung der technischen und organisatorischen Datensicherungsmaßnahmen bei Landratsämtern	31
3.5.5	Einsichtnahme in Studentenkarteien	21	3.11.5 Prüfung der organisatorischen Datensicherungsmaßnahmen der Studentenzentrale einer Fachhochschule	31
3.5.6	Abiturientenbefragung	21		
3.6	Statistik und Planung	21		
3.6.1	Übermittlung und Nutzung von Statistikdaten für sonstige Verwaltungszwecke	21		
3.6.2	Nutzung von Verwaltungsdaten für Planungszwecke	22		

	Seite	
3.11.6 Grundsätze für die Verarbeitung von Dateien mit personenbezogenen Daten	31	tungen an andere Datenschutz-Kontrollinstanzen, die für die Erledigung zuständig sind, die Versendung von Informationsmaterial und nicht zuletzt die Weiterführung des Datenschutzregisters (Dateienregisters) sowie Auskünfte aus diesem Register.
3.11.7 Überlegungen zur ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen	32	
3.12 Technische Einzelfragen	32	Der vorliegende Tätigkeitsbericht berücksichtigt diese Gliederung, wobei der 3. Komplex nur im Rahmen der Vorbemerkung (Teil 1) Erwähnung findet. Daß diese an sich unproblematische Tätigkeiten eine ganz erhebliche Arbeitslast in einer personell recht sparsam ausgestatteten Dienststelle mit sich bringen, sei an dieser Stelle vermerkt. Auch diese Arbeiten haben für die Beziehung Landesbeauftragter für den Datenschutz/Staatsbürger besondere Bedeutung.
3.12.1 Temporäre Dateien	32	
3.12.2 Datenschutzgerechte Papier- und Aktenvernichtung	33	
3.12.3 Anforderungen an ein rechnergesteuertes Zugangskontrollsystem	33	
3.13 Mitarbeit in ADV-Benutzer-Arbeitskreisen	33	Die Darlegungen zu 1. (s. a. Teil 2) sollen auch rechtspolitisch wichtige Fragen aufzeigen und zur Diskussion über die Novellierung des Datenschutzrechts beitragen. Da die angesprochenen Fragen noch in der Diskussion sind, soll hier nur die Thematik angesprochen werden.
3.13.1 Mitarbeit in der Benutzervereinigung SCOUT e. V.	33	
3.13.2 Mitarbeit in der Benutzervereinigung GUIDE	34	
4. Datenschutz beim Bayerischen Rundfunk	34	Die Ausführungen zu 2. setzen teilweise die Behandlung der in den ersten beiden Tätigkeitsberichten angesprochenen Einzelfragen fort und verweisen insoweit auf die Tätigkeitsberichte I und II. Erst im Laufe des Jahres 1980 aufgetretene, rechtliche wie technisch-organisatorische Einzelfragen werden in diesem Abschnitt abgehandelt (Teil 3 dieses Tätigkeitsberichts). Schließlich ist für eine allgemeine Befassung mit Datenschutzfragen auch auf die Tätigkeitsberichte des Bundesbeauftragten und der Datenschutzbeauftragten der anderen Bundesländer (mit Ausnahme von Hamburg, das 1980 noch kein Landesdatenschutzgesetz und keinen Datenschutzbeauftragten hatte) hinzuweisen.
Anhang 1		
Rechtliche Grundlagen des Datenschutzes in Bayern	36	
1.1 Vorschriften	36	
1.2 Wesentlicher Inhalt der Datenschutzgesetze	36	
Anhang 2		
Anschriften der Datenschutz-Kontrolle	37	
Anhang 3		
Stichwortverzeichnis	38	1.2 Zur Lage
1. Vorbemerkung		Stärker noch als in den beiden vorhergehenden Berichtszeiträumen begann sich im Jahre 1980 abzuzeichnen, was sinnvoller Datenschutz ist und was nicht; deutlich zeigten sich die Schwierigkeiten beim Vollzug der bestehenden Datenschutzgesetze:
1.1 Übersicht		– Sie sollen die Individualsphäre des Staatsbürgers schützen, ohne rechtswidrig Handelnde zu begünstigen,
Im Berichtsjahr 1980 zeigte sich deutlich, daß sich meine Tätigkeit in drei Gruppen unterteilen läßt:		– sie sollen die Verwaltung bestimmen, Zurückhaltung bei der Erhebung und Übermittlung von Daten zu üben, ohne ihre Wirksamkeit zu beeinträchtigen,
1. In Fragen, die grundsätzliche Bedeutung haben und Fragen, die aufgrund geltenden Rechts nicht zweifelsfrei oder nicht zufriedenstellend zu beantworten sind, deshalb eine Weiterentwicklung des Datenschutzrechts erforderlich erscheinen lassen und damit in die Zukunft greifen. Hierzu rechnen auch Probleme, die auf technischen Neuerungen beruhen.		– sie sollen das Datenbewußtsein von Bürgern und Verwaltung formen, ohne unnötige Besorgnisse auszulösen.
2. Fragen, die auf Grund des geltenden Rechts zu beantworten sind, Nachforschungen und Ermittlungen auf Grund von Anfragen und allgemeinen Kontrollen bei bestimmten Dienststellen, oder Kontrollen, die gezielt auf einen bestimmten Sachverhalt abgestellt sind, soweit dabei nicht grundsätzliche Fragen aufgeworfen werden (s. o. 1.).		Zwischen diesen Gegensätzen bewegt sich der Datenschutz. Dem Datenschutzbeauftragten fällt dabei öfter die Rolle des Beraters als die des Kontrolleurs zu.
3. Routinearbeiten, insbesondere die Erledigung von einfach zu beantwortenden Anfragen, Weiterlei-		Die Kritik am Datenschutz nahm zu. Sie soll wie jede Kritik in einem demokratischen Staatswesen befruchtend wirken.
		Die Ausführungen im ersten und zweiten Tätigkeitsbericht zu den Aufgaben des Landesbeauftragten für den Datenschutz, zur Funktion des Tätigkeitsberichts

und zur Einrichtung der Geschäftsstelle darf ich für das Berichtsjahr 1980 wie folgt ergänzen:

1.2.1 Beirat

In der Besetzung des Beirats beim Landesbeauftragten für den Datenschutz ist folgende Änderung eingetreten:

Als neues stellvertretendes Beiratsmitglied für die Sozialversicherungsträger wurde Herr Direktor Schmaus anstelle des ausgeschiedenen stellvertretenden Mitglieds Dr. Günter Adelfinger benannt.

Der Beirat hat im Berichtsjahr viermal (Februar, März, Oktober, November) getagt. Er hat sich dabei im wesentlichen mit folgenden Fragen befaßt:

- Rasterfahndung,
- Ergebnis der Überprüfung der technischen und organisatorischen Sicherungsmaßnahmen in Rechenzentren durch den Landesbeauftragten für den Datenschutz,
- Vorberatung des 2. Tätigkeitsberichts des Landesbeauftragten für den Datenschutz,
- Unterrichtung über Beanstandungen (Art. 29 Abs. 5 Satz 2 BayDSG),
- Führung kriminalpolizeilicher Ermittlungsdateien,
- Speicherung, Löschung und Übermittlung von Daten des Verfassungsschutzes,
- Erhebung von Kosten für die Erteilung von Auskünften über gespeicherte Daten.

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

1.2.2 Personal der Geschäftsstelle

Die Arbeitsfähigkeit der Geschäftsstelle war durch den schon im 2. Tätigkeitsbericht angesprochenen Stellenmangel gekennzeichnet. Dazu kam – nach Besetzbarkeit einer dritten Stelle des höheren Dienstes und leihweisen Zurverfügungstellung je einer Stelle des gehobenen und des mittleren Dienstes – die Schwierigkeit, geeignete Mitarbeiter zu finden: Sie mußten neben zuverlässigen Kenntnissen und praktischen Erfahrungen in bestimmten, für die Datenschutzkontrolle wesentlichen Verwaltungsbereichen, gute Kenntnisse der Datenverarbeitung im öffentlichen Dienst besitzen.

Dank der Unterstützung durch das Bayer. Staatsministerium der Justiz konnte die dritte Stelle des höheren Dienstes Mitte des Jahres 1980 mit einem Beamten besetzt werden, der die erforderlichen Spezialkenntnisse aus dem Bereich der Justiz- und Sicherheitsbehörden sowie in Datenschutzrecht und Datenverarbeitung mitbringt. Die geliehene dritte Stelle des gehobenen Dienstes konnte mit einem Fachmann aus dem Bereich der Kommunalverwaltung und kommunalen Datenverarbeitung besetzt werden. Es bleibt zu hoffen, daß die zur Unterstützung der Referenten dringend erforderlichen weiteren Sachbearbeiter aufgrund des neuen Haushaltes 1981/82 noch im Jahr 1981 eingestellt werden können. Voraussetzung dafür ist, daß die entsprechenden Stellen schon ab Inkraft-

treten des Haushalts und nicht nur in der jeweiligen Eingangsstufe der Laufbahngruppe besetzbar sind. Der Personalstand meiner Geschäftsstelle wird auch nach der von mir angestrebten Personalmehrung im Vergleich zu den Geschäftsstellen anderer Beauftragter für den Datenschutz bescheiden bleiben. .

1.2.3 Datenschutzregister

Im Tätigkeitsbericht des vergangenen Jahres wurde ausführlich über den Aufbau des Datenschutzregisters berichtet. Die jährlich zu veröffentlichende Übersicht über das Datenschutzregister hatte am Ende des Jahres 1979 8286 Dateieinzelmeldungen von insgesamt 2537 speichernden Stellen enthalten.

Nachdem zum 1. 1. 1980 eine Reihe von Verwaltungsgemeinschaften aufgelöst bzw. viele Mitgliedsgemeinden aus Verwaltungsgemeinschaften entlassen wurden, war für den Berichtszeitraum mit einem weiteren Anwachsen der Dateimeldungen zu rechnen. Hinzu kommt, daß der Einzug der automatisierten Datenverarbeitung in die Rathäuser kleinerer und mittlerer Gemeinden weiter anhält. Durch gezielte Umfrageaktionen bei den Landratsämtern wurde außerdem versucht, die Zahl der öffentlichen Stellen, die personenbezogene Daten in automatisierten Verfahren verarbeiten und bisher nicht zum Datenschutzregister gemeldet haben, zu verringern. Dies trifft vor allem für den Bereich der Gemeinden und Zweckverbände zu.

Mit dem Landesverband der Ortskrankenkassen wurden die Dateimeldungen der 39 Allgemeinen Ortskrankenkassen in Bayern abgestimmt. Mit Hilfe des Landesverbandes der Innungskrankenkassen wurden in ähnlicher Weise die Meldungen der Innungskrankenkassen auf Vollständigkeit überprüft.

Am 13. Oktober 1980, dem Redaktionsschluß für die Übersicht über das Datenschutzregister, die am 21. November 1980 als Anlage der Nr. 47 des Bayer. Staatsanzeigers veröffentlicht wurde, hatten insgesamt 3049 speichernde Stellen 10 145 Einzeldateien zum Datenschutzregister gemeldet. Diese Zahlen bedeuten einen Zuwachs gegenüber dem Vorjahr von 25 Prozent bei den Dateimeldungen und von ca. 20 Prozent bei den speichernden Stellen. Die 2. Übersicht hat einen Umfang von 256 Seiten. Im Berichtsjahr wurden auf Sammel- und Einzelanforderungen über 700 „Übersichten“ versandt.

Die im Berichtszeitraum durchgeführten Einzelprüfungen im Kommunalbereich zeigten, daß ca. 15 Prozent der automatisiert geführten Dateien nicht zum Datenschutzregister gemeldet waren. Dieser Erfahrungswert läßt vermuten, daß sich die Zahl der Meldungen auch 1981 erhöhen wird. So beläuft sich die Zahl der nach dem Redaktionsschluß für die Übersicht über das Datenschutzregister bis zum Ende des Berichtsjahres eingegangenen Nachmeldungen auf etwa 200.

Trotz zahlreicher Aufklärungsaktionen und der noch ausführlicher gestalteten Ausfüllanleitung für die Meldungen waren wieder zahlreiche Rückfragen erforderlich. Vor allem wurde festgestellt, daß sehr viele Meldungen unvollständig ausgefüllt werden und unklar ist, wann eine Datenübermittlung vorliegt. Häufig

wurde fälschlicherweise die Bescheiderteilung an einen Betroffenen als Datenübermittlung angegeben.

Der praktische Wert des mit viel Mühe und Geduld in meiner Geschäftsstelle eingerichteten Datenschutzregisters und der über dieses Register jährlich mit erheblichem Aufwand zu veröffentlichenden „Übersicht“ ist schwer abschätzbar. Ohne Zweifel groß ist der Wert für meine Geschäftsstelle, da Register und Übersicht unverzichtbare und zuverlässige Hilfsmittel für Auskünfte und Kontrollen sind. Die Zahl der im Berichtsjahr versandten Übersichten zeigt, daß das Interesse der Öffentlichkeit an der Feststellung der bei Behörden gespeicherten Daten zunimmt. Weitere Einzelheiten zum Datenschutzregister sind im 1. und 2. Tätigkeitsbericht dargestellt (I Nr. 2.4, Seite 6, und II Nr. 2.4, Seite 11 und 12 der Landtagsdrucksachen).

1.2.4 Konferenzen der Datenschutzbeauftragten

Die Konferenz der Beauftragten für den Datenschutz der Länder und des Bundes sowie der Datenschutzkommission in Rheinland-Pfalz stand vom Herbst 1979 bis Herbst 1980 unter dem Vorsitz des Bayer. Landesbeauftragten für den Datenschutz in München. Ab Dezember hat der Berliner Datenschutzbeauftragte den Vorsitz übernommen. Sie hat im Jahr 1980 insgesamt viermal getagt.

Aus den behandelten Themen sind hervorzuheben:

- Sicherheitsbereich
- Meldewesen
- Mitteilungen in Strafsachen (MiStra)
- Zentraldateien der Staatsanwaltschaften
- Neue Medien
- Sozialbericht für Suchtkranke
- Sozialgesetzbuch
- Statistik

Die Konferenz erarbeitete gemeinsame Stellungnahmen zu

- Rasterfahndung
- Melderechtsrahmengesetz
- Bundespersonalausweisgesetz
- Anordnung über Mitteilungen in Strafsachen (MiStra)
- Neue Medien

Zu Einzelheiten wird auf Teil 3 dieses Berichtes verwiesen.

Bei der vom Bundesbeauftragten für den Datenschutz einberufenen 3. Kooperationssitzung des Bundes und der Länder wurden neben zahlreichen Einzelfragen auch Überlegungen für eine Novellierung des BDSG erörtert.

1.2.5 Anrufung des Landesbeauftragten für den Datenschutz, Auskunft „über die gespeicherten Daten“

Auch im 3. Jahr meiner Tätigkeit liegt bei den Anfragen von Bürgern die Fragestellung „Wo erhalte ich Auskunft über alle zu meiner Person gespeicherten Daten?“ an der Spitze.

Ich sehe es deshalb als notwendig an, in diesem auch für die Öffentlichkeit bestimmten Bericht klarzustellen, daß es in der Bundesrepublik keine Stelle gibt, die eine Übersicht darüber besitzt, ob und welche Daten über den einzelnen bei welcher Stelle gespeichert sind. Die Existenz einer solchen Stelle wäre selbst eine Bedrohung des Persönlichkeitsrechts aller betroffenen Personen im höchsten Ausmaß, da diese Stelle dann „alles“ über den einzelnen wüßte – zumindest all das, was Behörden oder Firmen in Dateien speichern. Diese Beurteilung würde auch für eine solche zentrale Stelle gelten, die zwar nicht jedes Einzeldatum kennen würde, jedoch die Fundstellen der einzelnen Daten zur Verfügung hätte.

Es gibt nicht nur keine Stelle, die dem Betroffenen darüber Auskunft geben kann, bei welchen aus der Vielzahl der Behörden Daten über ihn gespeichert sind. Auch der Bayerische Landesbeauftragte für den Datenschutz kann diese Auskunft nicht erteilen. Er kann dem Auskunftsuchenden lediglich seine Hilfe anbieten festzustellen, welche Stellen der bayerischen Behörden möglicherweise über ihn Daten gespeichert haben könnten. Alle bayerischen Behörden müssen nämlich ihre automatisiert gespeicherten Datensammlungen an das Datenschutzregister melden, das in der Geschäftsstelle des Landesbeauftragten geführt wird. Das Register ist demnach nur ein Verzeichnis dieser Datensammlungen und enthält keinerlei personenbezogene Daten von Bürgern. In dieses Register kann jedermann Einsicht nehmen. Der Inhalt des Registers wird durch die oben genannte „Übersicht“ erschlossen. Durch einen Blick in die Übersicht kann möglicherweise geklärt werden, bei welcher „speichernden Stelle“ Datenschutzrechte geltend zu machen sind. Solche Datenschutzrechte sind Auskunfts-, Berichtigungs-, Sperrungs- und Löschungs-Rechte sowie die Ansprüche auf Unterlassung, Beseitigung oder Schadensausgleich. Um Interessenten, die nicht ohne weiteres Einsicht in das Register nehmen können, weil sie nicht in München und Umgebung wohnen, einen Ausgleich zu bieten, versende meine Geschäftsstelle auf Anforderung die „Übersicht“ über den Inhalt des Datenschutzregisters oder Auszüge aus dem Register kostenlos.

2. Grundsätzliche Fragen und neue Probleme

2.1 Fortentwicklung des Datenschutzrechts

Das Datenschutzrecht hat sich im Jahre 1980 zunächst in verschiedenen bereichsspezifischen Vorschriften fortentwickelt:

– Das Gesetz zur Änderung des Gesetzes über Personalausweise vom 6. März 1980 (BGBl. I S. 270), das die Grundlage für die Einführung eines maschinenlesbaren Personalausweises schuf, enthält gleichzeitig Verwendungsbeschränkungen und ein Nutzungsverbot für die Seriennummer des Ausweises (Einzelheiten siehe Tätigkeitsbericht II S. 9 und 10). Außerdem bestimmt § 3 Abs. 3 dieses Gesetzes: „Eine zentrale, alle Seriennummern umfassende Speicherung darf nur bei der Bundesdruckerei und ausschließlich zum Nachweis des Verbleibs der Ausweise erfolgen. Die Speicherung der übrigen, in § 1 Abs. 2 genannten Angaben bei der Bundes-

druckerei ist unzulässig.“ Der Gesetzgeber hat mit- hin die Speicherung der Daten des Personalaus- weises bei der Bundesdruckerei – mit Ausnahme der Seriennummer – verboten. Diese Einschränkung ist aus der Sicht des Datenschutzes zu be- grüßen.

Ungeachtet dessen schlug die Bundesdruckerei ein Herstellungsverfahren vor, das eine Speicherung von Personalausweis-Daten erforderlich macht. Er- klärt wird dazu, daß beabsichtigt sei, die Personalausweis-Daten nur für eine kurze Dauer, während des Herstellungsverfahrens, zu speichern.

Die Einführung dieses Verfahrens wäre wegen der vorgesehenen Speicherung gesetzwidrig. Ich halte es für sehr problematisch, hier nur einen formellen Gesetzesverstoß anzunehmen, denn nach der bis- herigen Gestaltung des Verfahrens ist ein kurzfr- istiges Speichern nur sichergestellt, wenn die Daten tatsächlich nach kurzer Zeit wieder gelöscht wer- den. Die Kürze der Speicherungszeit hängt also von der Umsetzung der genannten Absicht der Bun- desdruckerei ab. Allein durch Untätigkeit, also durch Nicht-Löschen der Daten, würde eine längere oder dauernde Speicherung bewirkt. Für den Über- gang von kurzzeitiger zu längerer oder dauernder Speicherung wären zusätzliche technische Einrich- tungen oder Datenverarbeitungsprogramme nicht erforderlich.

- Das Melderechtsrahmengesetz vom 16. August 1980 (MRRG, BGBl. I S. 1429) hat aus der Sicht des Datenschutzes Fortschritte hinsichtlich der Aufga- bendefinition der Meldebehörden, der Begrenzung der dort zu speichernden Daten und der Konkreti- sierung von Datenübermittlungen gebracht. Wäh- rend frühere Entwürfe für ein Bundesmeldegesetz ein umfassendes Einwohner-Informationssystem er- möglichen wollten, das Daten aus allen denkbaren kommunalen Verwaltungsbereichen enthalten und mit Hilfe des „Personenkennzeichens (PK)“ eine Verknüpfung zu weiteren Daten der öffentlichen Verwaltung schaffen sollte, wurde das nun erlas- sene MRRG – in Änderung der Zielsetzung – auch als bereichsspezifische Datenschutzregelung kon- zipiert. Der Gesetzgeber wollte nun bewußt nicht mehr die Basis für ein allgemeines Einwohner-In- formationssystem legen.

Um so gespannter werden nun die Entwürfe für die noch zu erlassenden Landesmeldegesetze erwar- tet. Forderungen aus der Sicht des Datenschutzes richten sich auf:

- Die Konkretisierung der Aufgaben der Meldebe- hörden, die zusammen mit der Beschränkung der zu speichernden Daten letztlich darüber entschei- den, ob die vom MRRG vorgezeichnete Abkehr von einem allgemeinen Informationssystem in die Praxis umgesetzt wird,
- die Vermeidung von solchen Ordnungsmerkma- len, die durch ihre Funktion wie das früher vor- gesehene Personenkennzeichen als Verknüp- fungsmerkmal zu anderen Behördenbereichen oder gar zum nichtöffentlichen Bereich dienen könnten,

- die datenschutzgerechte Ausgestaltung der fest- zulegenden Datenübermittlungen,
- die Ausschöpfung von Möglichkeiten, die Schutz- rechte der Bürger zu verbessern und
- die Gestaltung des landeseinheitlichen Verfah- rens für das Meldewesen.

- Das Sozialgesetzbuch – Verwaltungsverfahren –, 10. Buch vom 18. August 1980 (SGB X, BGBl. I S. 1469), enthält in Artikel II, § 28 eine Neufassung des „Sozialgeheimnisses“ in § 35 SGB I und in Art. 1, 2. Kapitel, §§ 67 bis 85, bereichsspezifische Vorschriften über den „Schutz der Sozialdaten“ (siehe auch unten Nr. 3.4.1.). Hier ist die zweifellos zu knappe Regelung des früheren § 35 SGB I in eine Vielzahl konkret formulierter Offenbarungs- befugnissen aufgelöst worden, die zwar zur Klar- stellung beitragen, jedoch keine wesentlichen Über- mittlungsbeschränkungen gegenüber der bisher- igen Praxis enthalten. Im übrigen sind einzelne Vor- schriften unzureichend aufeinander abgestimmt, so daß erneut Diskussionen um mehr oder weniger datenschutzfreundliche Gesetzesauslegungen aus- gelöst werden.

Die Fortentwicklung des Datenschutzrechts hat im Berichtsjahr auch die Schwierigkeiten der Verbesse- rung des Datenschutzes durch bereichsspezifische Regelungen deutlich werden lassen. Ich halte es da- her für verfehlt, die Fortentwicklung überwiegend auf bereichsspezifische Regelungen gründen zu wollen. Es hat sich vor allem gezeigt, daß in spezielle Rege- lungen spezielle Interessen wesentlich stärker ein- fließen als in allgemeinen Regelungen, wie BDSG oder BayDSG. Der Novellierung des BDSG, die be- reits seit längerem erörtert wird, und die für die Ent- wicklung des BayDSG wiederum maßgeblich ist, dürfte daher wesentliche Bedeutung für die Fortentwicklung des Datenschutzrechts zukommen. Ich befürworte eine gründliche, nicht unter Zeitdruck stehende Aus- einandersetzung mit allen entwicklungsbedürftigen Punkten des Gesetzes. Für den Datenschutz bei öf- fentlichen Stellen hielte ich hierbei für wesentlich:

- Das Gesetz möglichst unabhängig von gegenwärtigen organisatorischen oder technischen Voraus- setzungen zu formulieren. Probleme erzeugen der- zeit die geltenden Datei-, Datenverarbeitungs- und Übermittlungsbegriffe (siehe auch Tätigkeitsbericht I Nr. 3.2, II Nr. 3.1.1, 3.1.8, 3.1.3),
- die Datenerhebung selbständiger zu regeln als bis- her (siehe II Nr. 3.1.4 und unten 2.3) und die Unzu- lässigkeit der Verarbeitung rechtswidrig erhobener Daten festzulegen,
- die Ausübung sämtlicher Schutzrechte, für den Be- troffenen von Kosten freizustellen (siehe II Nr. 3.1.10),
- die Vorzüge, die das später erlassene Bayer. Da- tenschutzgesetz gegenüber dem BDSG aufweist, in das BDSG zu übernehmen: Anspruch auf verschul- densfreien Schadensausgleich (Art. 13 BayDSG), auf Sperrung von Daten bei berechtigtem Interesse (Art. 10 Nr. 1 BayDSG), auf Unterlassung oder Be- seitigung (Art. 12 BayDSG), auf Zuweisung von Auf-

gaben durch Rechtsnorm als Voraussetzung der Zulässigkeit der Datenverarbeitung (Art. 16 Abs. 1, 17 Abs. 1, 18 Abs. 1 BayDSG), Anwendung der Datenübermittlungsregeln auf die Weitergabe zwischen verschiedenen Ämtern (Art. 17 Abs. 3 Satz 2 BayDSG) sowie zentrale jährliche Veröffentlichung einer Übersicht über sämtliche automatisierte Dateien anstatt verstreuter Veröffentlichungen in verschiedenen Amtsblättern (Art. 7 Abs. 3 BayDSG),

- klarere Formulierung der Zuständigkeit des Datenschutzbeauftragten für die Kontrolle der Einhaltung anderer Vorschriften über den Datenschutz (s. a. nachfolgend 2.2). Erstreckung seiner Kontrolle auf nichtöffentliche Stellen als Auftragnehmer öffentlicher Stellen bei der Erfüllung öffentlicher Aufgaben – soweit nicht die Kontrolle durch die Aufsichtsbehörden sichergestellt ist. Klarstellung der Kontrollzuständigkeit für Bund-Länder-Vereinigungen unter Berücksichtigung der verfassungsmäßigen Kompetenzverteilung zwischen Bund und Ländern.

Darüber hinaus können u. U. in einem besonderen Teil des BDSG, ähnlich einem Artikel-Gesetz, spezielle Verbesserungen einzelner Verwaltungsbereiche erzielt werden.

2.2 Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz

Nach Art. 28 Abs. 1 BayDSG überwacht der Landesbeauftragte für den Datenschutz „die Einhaltung des Datenschutzes bei allen öffentlichen Stellen“. Soll diese Bestimmung nicht einen erheblichen Teil ihrer Schutzfunktion für Bürger und Verwaltung verlieren, muß sie dahin verstanden werden, daß sie die Einhaltung „des Datenschutzes“ generell betrifft, also unabhängig davon, ob sich die jeweils einschlägigen Datenschutz- oder Verschwiegenheitsvorschriften im Datenschutzgesetz selbst oder in anderen Vorschriften finden. Andere Vorschriften sind zum Beispiel das Steuergeheimnis, das Sozialgeheimnis, die ärztliche Schweigepflicht und die sonstigen Schweigepflichten des § 203 Abs. 2 StGB. In einem konkreten Fall waren Daten aus der Datei einer nachgeordneten Behörde einem Ministerium übermittelt worden. Das Ministerium hatte die Daten bearbeitet und anschließend aus den Akten (also nicht mehr „aus einer Datei“) Angaben an eine nichtöffentliche Stelle übermittelt. Da auf die zweite Daten-Weitergabe das Bayer. Datenschutzgesetz mangels „Übermittlung aus einer Datei“ nicht anwendbar war, hat es der Beirat beim Landesbeauftragten für den Datenschutz in seiner Sitzung am 11. 3. 1980 einhellig begrüßt, daß diese Weitergabe vom Landesbeauftragten auf Grund des Art. 28 Abs. 1 BayDSG („... überwacht die Einhaltung des Datenschutzes bei allen öffentlichen Stellen“) anhand der allgemeinen Vorschriften über Geheimhaltung und Offenbarungsbefugnis geprüft werden konnte, so daß sich letzten Endes kein „datenschutzfreier“ Raum ergab.

Im übrigen ist eine Überdeckung des Bereichs der Kontrollzuständigkeit des Landesbeauftragten für den Datenschutz und der allgemeinen Rechtsaufsichtsbehörden vom Gesetzgeber gewollt. Beide Bereiche

konkurrieren nicht, sie ergänzen sich sinnvoll. Dies ist eine Erscheinung, die sich auch bei der Tätigkeit des Bayerischen Obersten Rechnungshofes ergibt.

2.3 Erhebung von Daten

Im Berichtszeitraum wurde erneut deutlich, daß die Auslegung des Art. 16 Abs. 2 BayDSG Schwierigkeiten bereiten kann. Insbesondere hat sich die Frage ergeben, ob Art. 16 Abs. 2 BayDSG auf jegliche Art der Datenerhebung anzuwenden ist oder nur auf die Erhebung solcher Daten beschränkt ist, die in Dateien gespeichert werden sollen. Hierzu habe ich folgende Auffassung vertreten:

Im Zeitpunkt einer Datenerhebung steht vielfach noch nicht abschließend fest, ob die Daten überhaupt oder eventuell nur zu einem Teil in Dateiform festgehalten werden sollen. Denkbar ist außerdem, daß die vorgesehene Art der Niederlegung der Daten nach deren Erhebung geändert wird. Eine Überprüfung der richtigen Anwendung des Art. 16 Abs. 2 BayDSG wäre stark erschwert, würde man Art. 16 Abs. 2 BayDSG nur auf in Dateien gespeicherte oder zu speichernde Daten anwenden. Im übrigen hinge die Anwendung dieser Vorschrift von subjektiven Vorstellungen des Datenerhebenden ab über die organisatorischen Abläufe und damit die weitere Verwendung der Daten. Damit bliebe diese Vorschrift vielfach wirkungslos.

Darüber hinaus ergibt sich sowohl aus dem Zweck des Art. 16 Abs. 2 BayDSG wie aus der Auslegung der im Bayerischen Datenschutzgesetz verwendeten Begriffe, daß diese Vorschrift wohl umfassender gesehen werden muß. Zweck des Art. 16 Abs. 2 BayDSG ist es, vorverlagerten Datenschutz zu sichern. Bereits die Erhebung von personenbezogenen Daten kann zu Gefährdungen für den einzelnen führen, auch wenn derartige Gefährdungen sich vielfach erst in der nachfolgenden Datenverarbeitung im Sinne der Legaldefinition des Art. 1 Abs. 1 BayDSG konkretisieren. In diesem Vorfeld der Datenerhebung wollte der Gesetzgeber bereits Schranken ziehen, um das durch überflüssig erhobene Daten möglicherweise entstehende Gefährdungspotential zu vermeiden. Diesen Zweck erreicht die Vorschrift jedoch nur, wenn grundsätzlich in allen Fällen der Erhebung personenbezogener Daten der Betroffene auf eine etwa bestehende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hingewiesen wird. Denn durch die Notwendigkeit eines derartigen Hinweises dürften in der Praxis unzulässige Datenerhebungen zurückgedrängt werden.

Darüber hinaus zeigt auch die Verwendung des Begriffes der Datenerhebung in Art. 16 Abs. 2 BayDSG, daß der durch Art. 1 Abs. 2 BayDSG beschriebene generelle Schutzbereich des Bayerischen Datenschutzgesetzes durch Art. 16 Abs. 2 BayDSG punktuell vorverlagert wird. Das Erheben von Daten, das nicht mit dem Erfassen von Daten gleichzusetzen ist, wird von dem im Bayerischen Datenschutz definierten umfassenden Begriff der Datenverarbeitung nicht umfaßt. Dies zeigen auch die entsprechenden Legaldefinitionen dieses Begriffes in Art. 1 Abs. 1 BayDSG wie der Begriffe Speichern, Übermitteln, Verändern und

Löschen in Art. 5 Abs. 2 BayDSG. Die Beschränkung des Anwendungsbereichs des Bayerischen Datenschutzgesetzes in Art. 1 Abs. 2, die sich ausschließlich auf die dort genannten Formen der Datenverarbeitung bezieht, läßt sich somit auf Art. 16 Abs. 2 BayDSG nicht ausdehnen. Dabei mag es dahinstehen, ob Art. 16 Abs. 2 BayDSG gesetzessystematisch an unglücklicher Stelle steht. Die Vorschrift entspricht wortgleich § 9 Abs. 2 BDSG, der – wie bekannt – im Regierungsentwurf des Bundesdatenschutzgesetzes zunächst nicht enthalten war. Aus dieser Entstehungsgeschichte ist die räumliche Stellung der Vorschrift des § 9 Abs. 2 BDSG im zweiten für die öffentliche Verwaltung geltenden Abschnitt des Bundesdatenschutzgesetzes und damit wiederum die Zuordnung als Abs. 2 zu der entsprechenden Vorschrift des Bayerischen Datenschutzgesetzes zu verstehen. Rückschlüsse aus dieser räumlichen Zuordnung auf die Auslegung dieser Bestimmung erscheinen mir daher im Hinblick auf das Vorstehende unzulässig. Art. 16 Abs. 2 BayDSG gilt somit für jedes Erheben personenbezogener Daten Betroffener. Für die Anwendbarkeit dieser Vorschrift ist es nicht notwendig, daß die Erhebung der Daten von vorneherein für deren Speicherung in einer Datei geschieht.

Für die dringend erforderliche Überprüfung der vielfältigen im Bereich der bayerischen öffentlichen Verwaltung verwendeten Formblätter und deren Umgestaltung im Hinblick auf die Forderung des Art. 16 Abs. 2 BayDSG ist es daher nicht notwendig, zunächst festzustellen, ob die mit diesen Formblättern zu erhebenden Daten künftig in Dateien gespeichert werden sollen oder nicht.

2.4 Besondere datenschutzrechtliche Freigabe von neuen Verfahren der automatischen Datenverarbeitung

Trotz meiner Hinweise im 1. und 2. Tätigkeitsbericht (I: Tz. 2.2, II: Tz. 2.2.5) zeigte sich im Zuge der Datenschutzkontrolle im Berichtsjahr erneut, wie wenig bekannt ist, daß aufgrund Art. 26 Abs. 2 BayDSG eine besondere datenschutzrechtliche Freigabe der Speicherungs- und Übermittlungsdatensätze für neue oder wesentlich geänderte ADV-Verfahren erforderlich ist und daß diese Freigabe nicht identisch ist mit der ADV-technischen Freigabe nach Abschluß der Programmierung bzw. vor Übergabe des Verfahrens an die Fachabteilung.

Die datenschutzrechtliche Freigabe ist gemäß Art. 26 Abs. 4 BayDSG dem Landesbeauftragten für den Datenschutz „unverzüglich mitzuteilen“. Vor dem erstmaligen Einsatz des Verfahrens erhält der Datenschutzbeauftragte außerdem die Meldung zum Datenschutzregister gem. Art. 7 BayDSG.

Sowohl die datenschutzrechtliche Freigabe durch die oberste Dienstbehörde als auch die Mitteilung dieser Freigabe an den Landesbeauftragten für den Datenschutz sollen eine möglichst frühzeitige Überprüfung der zur Programmierung vorgesehenen Speicherungs- und Übermittlungsdatensätze möglich machen. Die Berücksichtigung von Bedenken der obersten Dienstbehörde oder des Landesbeauftragten für den Daten-

schutz wird erheblich schwieriger, je weiter ein ADV-Verfahren bereits fertiggestellt ist. Nach Fertigstellung besteht die Gefahr, daß Anregungen oder Bedenken nicht mehr berücksichtigt werden. Diese Auslegung der datenschutzrechtlichen Freigabe ist gemäß Art. 28 Abs. 6 BayDSG im Beirat eingehend vorberaten worden. Die Vertreter der kommunalen wie der staatlichen Seite bestätigten die Richtigkeit dieser Auslegung.

2.5 Datenverarbeitung im Auftrag

Vor allem im Bereich der automatisierten Datenverarbeitung nehmen speichernde Stellen häufig die Unterstützung anderer öffentlicher oder privater Stellen in Anspruch. Zum Teil wird die gesamte ADV-technische Abwicklung „außer Haus“ gegeben, teils sind es einzelne Ausschnitte, wie z. B. Datenerfassung, Datenausgabe auf Mikrofilm oder Datenspeicherung, in manchen Fällen mit Ein- und Ausgabe über Endgeräte bei der speichernden Stelle. Aufgrund praktischer Erfahrungen sei auf folgendes Problem hingewiesen:

Der Auftraggeber kann dem Auftragnehmer die Weisung erteilen, die in seinem Auftrag verarbeiteten Daten an eine andere Stelle zu übermitteln. Es ist denkbar, daß die Weisung nicht nur für Einzelfälle, sondern generell, ohne besondere zeitliche Begrenzung für alle Übermittlungen gegeben wird, die unter bestimmten Voraussetzungen durchzuführen sind („Daueraufträge“). Eine solche Voraussetzung könnte die Anforderung von Daten durch eine dritte Stelle sein. Dabei kann problematisch werden, daß vor jeder konkreten Datenübermittlung eine Prüfung und eine Entscheidung durch die abgebende speichernde Stelle nicht mehr stattfindet.

Ist außerdem der Auftragnehmer eine Stelle, die solche Aufgaben für eine Vielzahl gleichartiger öffentlicher Stellen durchführt, so bedeutet dies, daß faktisch eine Datenstelle anstatt einer Vielzahl öffentlicher Stellen tätig wird. Zwar wird, um einen gültigen Auftrag zur Datenübermittlung annehmen zu können, die an der Übermittlung interessierte Stelle zunächst die Vielzahl der Behörden (= speichernden Stellen) zur Zustimmung in die künftige Abgabe von Daten durch den Auftragnehmer „auf Abruf“ bewegen müssen. Sind die entsprechenden Zustimmungen jedoch eingeholt, so kann der Empfänger der Datenübermittlung von einer einzigen Stelle einfach und schnell Daten einer Vielzahl über das Land verteilter öffentlicher Stellen erhalten.

Insbesondere derartigen „Daueraufträgen“ zur Weitergabe von Daten durch solche zentrale Auftragnehmer können aus der Sicht des Datenschutzes Bedenken begegnen.

Eine Übermittlung von Angaben über Gemeindebürger kann deren Interessen grundsätzlich berühren. Die Gemeinde wird daher solche Interessen bei ihrer Entscheidung über die Weitergabe berücksichtigen. Dabei ist einer durchaus rechtmäßigen Eigenwilligkeit einzelner Gemeinden ein erheblicher Spielraum eingeräumt, so daß Gemeinde oder Gemeinderat bei Ermessensentscheidungen über Datenüber-

mittlungen im Interesse der Bürger Zurückhaltung üben können. Ist die Aufgabenentwicklung dagegen bei einer einzigen Stelle konzentriert, kann dieser Spielraum taktisch verlorengehen. Beim Anschluß an ein allgemeines ADV-Verfahren kann

- von einem auf die Interessen der Mehrheit der Benutzer abgestellten Angebot des Auftragnehmers, Daten an einen bestimmten Empfänger zu übermitteln,
- von dem Wegfall des eigenen Übermittlungsaufwands bei der Gemeinde und
- von dem gleichförmigen Verhalten anderer angeschlossener Gemeinden

ein erheblicher Anpassungsdruck ausgehen. Die Tatsache der Übermittlung von Daten der Gemeindeglieder kann dadurch vorrangig durch die Interessen des Datenempfängers beeinflußt werden.

Ich bin der Ansicht, daß Bedenken, die sich hieraus ergeben können, dadurch begegnet werden muß, daß insbesondere diejenigen Stellen, die den Vorteil der Datenkonzentration beim zentralen Auftragnehmer nutzen wollen, das Selbstverwaltungsrecht der Auftraggeber mit besonderer Sorgfalt behandeln müssen.

Zu Verträgen über Auftragsdatenverarbeitung haben sich im übrigen erste Erfahrungen ergeben:

- Die weitere Übertragung von Aufträgen oder Auftragsteilen an Subunternehmer setzt die Einwilligung des Auftraggebers zum konkreten Unterauftrag voraus. Der Auftraggeber kann sonst in der Regel nicht seine Pflicht zur sorgfältigen Auswahl des Auftragnehmers erfüllen (Art. 3 Abs. 1 Satz 2 BayDSG, § 8 Abs. 1 Satz 2 BDSG).
- Der Auftraggeber muß in ausreichendem Umfang Weisungen erteilen, d. h. er muß die auszuführenden Arbeiten so beschreiben, daß Entscheidungen, insbesondere Ermessensentscheidungen, vom Auftragnehmer nicht mehr getroffen werden müssen, um den Auftrag auszuführen. Dies gilt beispielsweise auch für den jeweils erforderlichen Standard der Datensicherung.
- Die Datenschutzgesetze haben erkennbar das Ziel, ein Ausweichen der öffentlichen Verwaltung in den privatrechtlichen Bereich zu erschweren, um die Verantwortlichkeiten nicht zu verwischen. In den Vorschriften über die Auftragsdatenverarbeitung (Art. 3 BayDSG und § 8 BDSG) kommt dies durch die Betonung der sorgfältigen Auswahl des Auftragnehmers „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen“ zum Ausdruck.
- Vereinbarungen zwischen Auftraggeber und Auftragnehmer müssen deshalb m. E. sicherstellen, daß sich die Datenschutzsituation der Betroffenen durch die „Verarbeitung außer Haus“ gegenüber der Verarbeitung bei der öffentlichen Stelle selbst nicht verschlechtert. Probleme können sich zum Beispiel dann ergeben, wenn die Datenverarbei-

tung aus einem durch § 203 StGB geschützten Bereich zu einem Auftragnehmer verlagert wird, für den diese Bestimmung nicht gilt.

2.6 Neue Medien – Überblick

Meine besondere Aufmerksamkeit gilt den Datenschutzproblemen, die bei Einführung der Neuen Medien auftreten können. Die Speicherung umfangreicher Daten über Art und Umfang der Benutzung der durch die Neuen Medien angebotenen Dienste schafft die grundsätzlichen Voraussetzungen zur Erstellung tiefgreifender Persönlichkeitsprofile. Damit könnte der vielbeschworene „Gläserne Mensch“ Wirklichkeit werden. Dies gilt es zu verhindern. Bereits bei Durchführung der Pilotprojekte muß deshalb der Datenschutz ausreichend berücksichtigt werden, um den Gefährdungen für die Teilnehmer rechtzeitig zu begegnen. Hierauf sollten auch die vorgesehenen wissenschaftlichen Begleituntersuchungen auf den Themenbereich Datenschutz erstreckt werden. Die für das Pilotprojekt federführende Bayerische Staatskanzlei hat mir zugesichert, mich bereits an den Vorbereitungen für das Pilotprojekt rechtzeitig und ausreichend zu beteiligen.

Eine ausführlichere Darlegung der mit den Neuen Medien verbundenen Datenschutzprobleme und der möglichen Lösungsansätze findet sich in Nr. 3.9 dieses Tätigkeitsberichts.

2.7 Technische Zukunftsfragen

Die Konzeption unserer heutigen Betriebs- und Standardsoftware-Systeme stammt aus einer Zeit, in der die Forderung nach dem technischen Datenschutz nur eine nachrangige Bedeutung hatte. Die Hersteller werden deshalb zukünftig mehr Gewicht auf die Realisierung von datensicherungsunterstützenden Funktionen in ihrer Hard- und Software legen müssen.

Nicht zuletzt durch die Explosion der Personalkosten bieten die Hersteller von EDV-Anlagen sogenannte Fernwartungsdienste an. So sehr diese Entwicklung von der Seite der Wirtschaftlichkeit und der Effizienz der Datenverarbeitung her zu begrüßen ist, um so dringlicher müssen hier die Datenschutzerfordernisse an derartige Systeme gesehen werden. Im nächsten Tätigkeitsbericht werden hierüber Einzelheiten zu berichten sein.

Rechnerverbund und Datenfernverarbeitung, Schlagworte aus dem Anfang der 70er Jahre, bergen zwar Gefahren in sich, die „Verdatung“ der Bürger zu beschleunigen, sollten jedoch nicht dramatisiert werden. Die Euphorie dieser Jahre ist nicht zuletzt wegen der rapiden Entwicklung auf dem Gebiet der Mikroprozessor-Technik am Abklingen. Wenn überhaupt im öffentlichen Bereich, so existieren Rechnerverbunde lediglich innerhalb eines Geschäftsbereiches. Die Datenfernverarbeitung bietet beim Online-Zugriff bei Ausnützung aller technischen Hilfsmittel manchmal sogar größere Sicherheiten, als wir es von der heute noch weitverbreiteten Stapelverarbeitung in unseren Rechenzentren gewöhnt sind.

3. Einzelfragen

3.1 Melde- und Standesamtswesen

3.1.1 Meldescheine

Im Berichtszeitraum wurde festgestellt, daß Beherbergungsbetriebe teilweise Meldescheine verwenden, in denen mehr Angaben erhoben werden, als im amtlichen Vordruck vorgesehen sind (Verordnung zur Durchführung des Meldegesetzes vom 24. Januar 1972, GVBl. S. 74). In einem Fall wurden Einzelangaben zur Ehefrau erfragt, die der amtliche Vordruck nicht enthält. Die ursprüngliche Annahme, daß lediglich noch alte Vordrucke „aufgebraucht“ würden, bestätigt sich dabei nicht: Auch der „neueste“ Vordruck einer Herstellerfirma ging über das amtliche Formular hinaus.

Ich bin der Ansicht, daß Behörden, für die Meldescheine in Beherbergungsbetrieben ausgefüllt werden müssen, verpflichtet sind sicherzustellen, daß auf diesem Wege nur die vorgeschriebenen bzw. die zur Erfüllung der durch Rechtsnorm zugewiesenen Aufgaben erforderlichen Angaben erhoben werden. Die Überprüfung ist noch nicht abgeschlossen.

Aus einer Eingabe wurde bekannt, daß für die Anmeldung bei Nebenwohnungen die selben Meldeformulare verwendet werden wie bei der Anmeldung für die Hauptwohnung, obwohl hierfür weniger Angaben erforderlich sind. Der Anmeldende wird nicht darauf hingewiesen, welche Angaben für die Nebenwohnung entfallen können. Es wird empfohlen, spätestens im Zuge der Neuordnung des Melderechts im Rahmen des neuen Landesmeldegesetzes hier für Klarheit zu sorgen.

3.1.2 Übermittlung von Anschriften aus dem Melderegister an Parteien

Zur gegenwärtigen Rechtslage verweise ich auf meine Ausführungen in den früheren Tätigkeitsberichten (I S. 13 Nr. 4.1.6, II S. 18 Nr. 4.1.1.5). Den Meldebehörden ist danach erlaubt, den politischen Parteien Auskunft über Namen und Anschrift von Wählern während eines halben Jahres vor der Wahl zu erteilen. Eine Auswahl der Wahlberechtigten darf (nur) nach Altersgesichtspunkten, wie z. B. Jungwähler oder Altwähler, vorgenommen werden.

Diese bisherige Praxis wurde nun auch durch das Mitte 1980 verkündete Melderechtsrahmengesetz des Bundes für das neue Melderecht gesetzlich vorgeesehen.

Obwohl die Datenübermittlung gegenwärtig durch Art. 24 Abs. 2 BayDSG (Übermittlungsvoraussetzung: „Öffentliches Interesse“) und den Auftrag der Parteien aus dem Grundgesetz, an der Willensbildung des Volkes mitzuwirken, für gedeckt erachtet wurde, ist im Zusammenhang mit der Bundestagswahl in Eingaben an den Landesbeauftragten für den Datenschutz wiederholt Beschwerde über die Verwendung der Anschriften aus dem Melderegister durch Parteien geführt worden. Die Adressenweitergabe wurde als bedenkliche Vermengung behördlicher Befugnisse zur Datenerhebung mit den Interessen der zur Bundestagswahl kandidierenden Parteien aufgefaßt.

Ich bin deshalb der Ansicht, daß den vom Bayer. Staatsministerium des Innern den Meldebehörden bekanntgegebenen Auflagen für die Weitergabe von Wählerdaten besondere Bedeutung zukommt: Darin war unter anderem empfohlen worden, an die Parteien nach Möglichkeit nicht Anschriftenlisten, sondern unmittelbar verwendbare Adreßaufkleber auszugeben. Die Datenempfänger waren darauf hinzuweisen, daß die übermittelten Daten nur für die Zwecke der jeweiligen Wahl verwendet werden durften, daß jede Weitergabe an Dritte zu unterbleiben habe und nach dem Wahltermin verbliebene Unterlagen zu vernichten seien. Eine Datenschutzkontrolle bei den Datenempfängern obliegt der jeweils zuständigen Datenschutzaufsichtsbehörde für nichtöffentliche Stellen, soweit Beschwerden eingehen.

3.1.3 Gruppenauskunft aus dem Melderegister an Verbände und Vereine

Der Bundesverband der Sozialversicherten e. V. ist 1980 — wie schon früher — an verschiedene Meldebehörden mit der Bitte herangetreten, ihm die Anschriften sämtlicher Angehörigen bestimmter Geburtsjahrgänge bekanntzugeben. Eine solche Datenübermittlung wäre nur zulässig, wenn sie im „öffentlichen Interesse“ läge (Art. 24 Abs. 2 BayDSG). Außerdem bedarf sie nach der Vollzugsbekanntmachung zum Bayer. Meldegesetz (MABl. 1978 S. 553, Nr. 3.3.1) der Zustimmung des Bayer. Staatsministeriums des Innern. Diese Zustimmung ist regelmäßig versagt worden, da kommerzielle Interessen — wie z. B. Mitgliederwerbung — ein „öffentliches Interesse“ nicht begründen. Darüber hinaus wäre die Auskunftserteilung schon deshalb unzulässig, weil mit den Anschriften aller Angehörigen bestimmter Geburtsjahrgänge weitaus mehr Daten gefordert wurden, als selbst nach dem Vortrag des Verbandes „erforderlich“ waren, nämlich auch die Anschriften aller nicht sozialversicherungspflichtigen Personen der bezeichneten Jahrgänge.

3.1.4 Weitergabe und Veröffentlichung von Angaben durch das Standesamt

Standesämter veröffentlichen seit langem Angaben über Geburten oder Verhelichungen u. ä., wenn die Betroffenen eingewilligt haben. § 104 der Dienstanzweisung für die Standesbeamten vom 24. 6. 1978 (Bundesanzeiger Nr. 123 a) regelt dieses Verfahren. Die von den Standesämtern verwendeten Vordrucke zur Aufnahme der Personenstandfälle enthalten in der Regel eine Einwilligungserklärung, die von den Beteiligten unterschrieben werden kann. Die bisher verwendeten Formblätter lösen in zweierlei Hinsicht Bedenken aus:

Bei der Veröffentlichung von Geburten in Amtsblättern oder Tageszeitungen wird zumindest teilweise so verfahren, daß neben dem Namen des Neugeborenen bei ehelichen Geburten der Namen des Vaters oder beider Eltern, bei nichtehelichen Geburten nur der Name der Mutter erscheint. Die listenmäßigen Übersichten in der Zeitung offenbaren in diesen Fällen also die Tatsache der nichtehelichen Geburt. Die Formulierung der Einwilligungserklärung umfaßt aber diese Offenbarung nicht. Die geschilderte Art

der Bekanntgabe der nichtehelichen Geburten erfolgt daher in der Regel ohne die erforderliche Einwilligung. Die Einwilligungsformel müßte dieser Problematik angepaßt werden.

Mit der Zunahme der Direkt-Werbung treten immer mehr Firmen an die Gemeinden heran, Anschriften der Eltern von Neugeborenen oder von Jungvermählten bekanntzugeben. Dabei handelt es sich nicht nur um Anbieter aus dem örtlichen Bereich, die solche Angaben auch aus Veröffentlichung in Zeitung oder Amtsblatt entnehmen könnten, sondern immer wieder auch um Anfragen von großen, bundesweit tätigen Firmen. Im Berichtszeitraum wurden auch Anfragen eines offenbar bundesweit tätigen Dienstes festgestellt, der solche Anschriften sammelt und an verschiedene interessierte angeschlossene Anbieter weitergibt. Ich glaube, daß die Eltern von Neugeborenen oder Jungvermählten die Einwilligung in die Veröffentlichung oder Weitergabe ihrer Anschrift allenfalls in dem Bewußtsein erteilen, daß diese für den örtlichen Bereich von Interesse ist. Es darf wohl angenommen werden, daß in vielen Fällen keine Einwilligung in die Übermittlung von Angaben an Stellen erteilt würde, die für das ganze Bundesgebiet zentral solche Anschriften sammeln. Gegen die Aufnahme in solche zentralen Datensammlungen bestehen zum Teil Vorbehalte der Betroffenen. Es kann nicht unterstellt werden, daß Einwilligungen hierzu in gleichem Umfang erteilt würden, wie die Zustimmung zur Veröffentlichung in der (örtlichen) Presse. Ich bin deshalb der Ansicht, daß die Einwilligungserklärungen der Standesämter den Verhältnissen, die sich in den letzten Jahren entwickelt haben, angepaßt werden müssen. Ausgangspunkt entsprechender Überlegungen könnte eine Unterteilung der Einwilligung in Fragen nach dem Einverständnis zur Veröffentlichung in der lokalen Presse und zur Übermittlung an überörtliche bzw. zentrale Adressendienste sein. Dabei wird nicht verkannt, daß auch ein zentraler Adressendienst theoretisch die Zeitung-Veröffentlichung der Personenstandsfälle aller Gemeinden der Bundesrepublik auswerten könnte. Abgesehen davon, daß die Durchführbarkeit einer solchen Maßnahme unwahrscheinlich erscheint, würde dies von Personen, die in die Veröffentlichung in der örtlichen Presse einwilligen, wohl in Kauf genommen werden. Sie brauchen meiner Ansicht nach aber nicht in Kauf zu nehmen, daß ein Standesamt, dem eine Einwilligung lediglich zur (örtlichen) Veröffentlichung erteilt wurde, die Angaben von sich aus an einen zentralen Adreßauswertungsdienst sendet.

3.2 Sicherheitsbereich

Im Jahr 1980 setzte sich die Datenschutzdiskussion besonders stark mit der Tätigkeit der Polizeibehörden auseinander. Schwerpunkte waren hierbei die Neukonzeption des Systems „INPOL“, die Neufassung der Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen und die sogenannte Rasterfahndung.

3.2.1 Rasterfahndung durch die Polizei

Mit Rasterfahndung werden Maßnahmen der Polizei umschrieben, die durch die Auswertung großer außer-

halb des polizeilichen Bereichs angefallenen Datenmengen auf bestimmte Verhaltensmuster (Raster) hin dem Aufspüren gesuchter Schwerverbrecher dienen sollten. Auf diese Weise wurden insbesondere die Daten der Kunden von Energieversorgungsunternehmen und von Telefoninhabern durchgesehen. Die dem Raster entsprechenden Personen wurden polizeilich überprüft. Soweit diese Überprüfung negativ war, wurden nach meinen Erkenntnissen auch die Daten dieser Personen, wie bereits zuvor die Daten der übrigen, gelöscht.

Die meisten Rasterfahndungen, die der Suche terroristischer Gewalttäter gedient haben, beruhten auf Beschlüssen des Ermittlungsrichters beim Bundesgerichtshof. Als Rechtsgrundlage für das Herausgabeverlangen von Daten bzw. für das Verlangen auf Auskunft wurden in den richterlichen Beschlüssen § 94 Strafprozeßordnung und § 12 des Gesetzes über Fernmeldeanlagen (FAG) genannt. § 94 Abs. 2 Strafprozeßordnung gestattet die Beschlagnahme von Gegenständen, die als Beweismittel für ein Strafverfahren von Bedeutung sein können. Die Bestimmung des § 12 FAG sieht für strafgerichtliche Untersuchungen ein Auskunftsverlangen über den Fernmeldeverkehr vor.

Für die Übermittlung der Daten an die Polizei ohne vergleichbare richterliche Beschlüsse wurde insbesondere § 24 BDSG herangezogen. Nach § 24 BDSG ist eine Übermittlung personenbezogener Daten u. a. zulässig, soweit diese zur Wahrung berechtigter Interessen der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange der jeweiligen Betroffenen nicht beeinträchtigt werden. Den Interessen der Allgemeinheit entspricht die Verfolgung terroristischer Gewalttäter und hierbei auch der Zugriff auf Datenmaterial privater Stellen. Dieser Zugriff muß sich allerdings auf die für eine konkrete Fahndungsmaßnahme erforderlichen Daten beschränken. Bei der Prüfung der schutzwürdigen Belange der Betroffenen ist grundsätzlich in jedem Einzelfall eine Interessenabwägung nach dem Verhältnismäßigkeitsprinzip vorzunehmen. Im Hinblick auf den Umfang der in Frage kommenden Datenbestände kann es dann vertretbar sein, von der Einzelfallprüfung abzusehen, wenn wegen des besonderen Gewichts der Interessen der Allgemeinheit an der Aufklärung schwerster Straftaten eine globale Abwägung der speichernden Stelle, ob schutzwürdige Belange der Betroffenen beeinträchtigt werden, genügen kann. Dies wird auch von der Sensibilität der zu übermittelnden Daten und der Art deren weiterer Verwendung abhängen. Um die Gefährdung für die Betroffenen so gering wie möglich zu halten, dürfen die Daten für keinen weiteren polizeilichen Zweck verwendet und müssen nach ihrer zweckbezogenen Auswertung umgehend gelöscht werden.

Die Datenschutzbeauftragten der Länder und des Bundes haben in ihrer Konferenz am 11. und 12. 2. 1980 auch Probleme der Rasterfahndung besprochen. Hierzu haben sie festgestellt, daß sich bei den bisher in der Zuständigkeit des jeweiligen Datenschutzbeauftragten geprüften Fällen keine Anlässe zu Beanstandungen ergeben hätten. Sie sind jedoch der An-

sicht, daß die als Rechtsgrundlagen für die Rasterfahndung genannten Bestimmungen den mit diesen Maßnahmen verbundenen Problemen nicht gerecht werden. Die große Zahl der einbezogenen Personen, die Menge der verarbeiteten Daten und die dank der veränderten Informationsmethode gegebenen vielfältigen Nutzungsmöglichkeiten zwingen zu präzisen, auf die Rasterfahndung abgestellte Regelungen. Ziel muß es hierbei sein, den Verhältnismäßigkeitsgrundsatz stärker zur Geltung zu bringen und insbesondere die Interessen Unverdächtiger zu schützen, soweit diese von den Fahndungsmaßnahmen betroffen werden.

Bei Schaffung entsprechender Regelungen wird zu prüfen sein,

- zu welchen Zwecken solche Fahndungsmethoden angewandt werden dürfen,
- welche tatsächlichen Voraussetzungen zu fordern sind,
- ob und in welchem Umfang bestimmte Datenarten nicht einbezogen werden dürfen (z. B. Sozial-, Gesundheitsdaten),
- inwieweit sichergestellt werden kann, daß die Daten grundsätzlich nicht zu anderen Zwecken als zu der jeweiligen Fahndung verwendet werden,
- welche verfahrensmäßigen Sicherungen hierzu zu fordern sind (z. B. Löschung, Dokumentation, Kontrolle),
- ob und in welchem Umfang den Datenschutzbeauftragten vor jeweiligen Maßnahmen der Rasterfahndung Gelegenheit zu rechtzeitiger Stellungnahme zu geben ist,
- wie die Kontrolle bei länderübergreifenden Fahndungsmaßnahmen sicherzustellen ist.

Bei meinen auf Bürgeranfragen hin durchgeführten Überprüfungen habe ich festgestellt, daß die im Zusammenhang mit der Rasterfahndung gewonnenen Daten bei den Polizeibehörden durchweg gelöscht sind. Auf die unmittelbare Löschung der Daten nach Zweckerreichung werde ich auch in künftigen vergleichbaren Fällen drängen.

Zweifelsohne ist mit der Einführung der Rasterfahndung eine neue Qualität möglicher Gefährdungen Unschuldiger entstanden. Das Risiko, als Unschuldiger in Verdacht zu geraten, ist sicher gestiegen. Dabei erscheint aus datenschutzrechtlicher Sicht besonders bedenklich, daß durch Maßnahmen der Rasterfahndung sogar eine größere Zahl Unschuldiger zumindest kurzzeitig in den Verdacht, schwere Straftaten begangen zu haben, geraten kann oder jedenfalls mit diesen in Verbindung gebracht wird. Die Bewertung eines Unschuldigen als Verdächtigen stellt für diesen ohne Zweifel einen schwerwiegenden Eingriff in seine Rechtsposition dar. Weil auch hierbei der Verhältnismäßigkeitsgrundsatz der Verhältnismäßigkeit zu beachten ist, dürfen derartige Eingriffe in die Rechte Betroffener nur zur Aufklärung ganz besonders schwerwiegender Straftaten vorgenommen werden. Außerdem darf das bei derartigen Aktionen angefallene Material nicht zur Ermittlung weiterer, unbedeutenderer Fälle

Verwendung finden. Nur mit einer umgehenden Löschung nach Durchsicht der angefallenen Daten für die Zwecke der Rasterfahndung können weitere daraus entstehende Gefahren reduziert werden. Selbst wenn die Daten der Unschuldigen umgehend gelöscht werden, können sich für diese Person weitere im Einzelfall nicht immer exakt abzuschätzende Nachteile schon dadurch ergeben, daß etwa Nachbarn oder Vermieter durch polizeiliche Befragungen von dem Verdacht Kenntnis erlangt haben. Darüber hinaus kann zumindest in ländlichen Gegenden an den auf Grund einer Rasterfahndung überprüften Bürgern ein (bleibender) Makel hängenbleiben, weil sich die beteiligten Polizeibeamten an den Vorgang erinnern. Gerade zu dieser Problematik haben mich einige Schreiben von Betroffenen erreicht.

3.2.2 Kriminalpolizeiliche Sammlungen (KPS)

Die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen und für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt sind unter Beteiligung der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz überarbeitet worden (vgl. S. 10 ff. des 2. Tätigkeitsberichts). Die Innenminister und Innensenatoren des Bundes und der Länder haben den Richtlinien in der zuletzt vorgelegten Fassung zugestimmt. Zu diesen Richtlinien stelle ich fest, daß einige der von den Datenschutzbeauftragten des Bundes und der Länder vorgetragenen Vorschläge übernommen worden sind und in anderen Punkten ein aus der Sicht des Datenschutzes akzeptabler Kompromiß gefunden worden ist. Insbesondere ist die Regelung für die Auskunft an den Betroffenen über die zu seiner Person gespeicherten Daten zu begrüßen, die klarstellt, daß Auskunft erteilt wird, wenn nicht die Belange des Bürgers im Einzelfall hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen. Gleichwohl halte ich, wie auch die anderen Datenschutzbeauftragten, in einer Reihe von Punkten Verbesserungen für geboten. Generell gilt es nun, die praktische Anwendung dieser Richtlinien aufmerksam zu verfolgen und aus den hierbei gewonnenen Erfahrungen Änderungsvorschläge zu erarbeiten.

Nach Mitteilung des Bayer. Staatsministeriums des Innern sollen die vorgenannten Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen die bisherigen bayerischen Richtlinien über kriminalpolizeiliche Sammlungen ablösen. Mit einem entsprechenden Erlaß sei nach landesbezogener Anpassung der Richtlinien im Laufe des Jahres zu rechnen. Es sei beabsichtigt, in diese neuen Richtlinien auch Bestimmungen aufzunehmen für die Errichtung und Führung von Dateien mit personenbezogenen Daten bei Dienststellen der bayerischen Polizei. Das Bayer. Staatsministerium des Innern hat mir zugesichert, eine Entwurfsfassung der neuen Richtlinien beizeiten zuzuleiten.

3.2.3 Sperrung von Daten bei der Polizei

Die im Bayer. Datenschutzgesetz in Art. 10 und Art. 20 vorgesehene Sperrung von Daten gilt grundsätzlich

auch für Polizeibehörden. In den automatisierten Verfahren des Bayer. Landeskriminalamts wird dem Erfordernis der Sperrung dadurch Genüge getan, daß die von der Sperrung betroffenen Daten in den aktuellen Datenbeständen gelöscht werden und die gesperrten Daten in eine eigene Datei der gesperrten Datensätze aufgenommen werden. Zu dieser Datei der gesperrten Datensätze haben die Polizeidienststellen trotz Anschlusses an die EDV-Anlage des Landeskriminalamts keinen Zugang. Diese Vorgehensweise bei der Sperrung von Daten entspricht grundsätzlich den Anforderungen des Datenschutzgesetzes. Es muß jedoch gewährleistet sein, daß auf die Datei der gesperrten Datensätze nur in dem in Art. 20 Abs. 2 Bayer. Datenschutzgesetz vorgesehenen Umfang zugegriffen wird. Ein darüber hinausgehender Zugriff, etwa für besondere Dienststellen oder im Einzelfall eingerichtete Sonderkommissionen, ist grundsätzlich unzulässig.

3.2.4 Löschung von Daten bei der Polizei

Das Bayerische Landeskriminalamt hat, worauf ich bereits in meinem zweiten Tätigkeitsbericht hingewiesen habe, spezielle Dienstkräfte mit der beschleunigten Bereinigung der kriminalpolizeilichen Sammlungen beauftragt. Bei einzelnen Überprüfungen konnte ich mich von dieser Tätigkeit überzeugen, die unter Beachtung der Bayerischen Richtlinien über Kriminalpolizeiliche Sammlungen erledigt wird. Allerdings habe ich in einem Fall festgestellt, daß eine Kriminalakte zwar entsprechend den vorgenannten Richtlinien bereinigt war, der in der Kriminalakte befindliche ed-Bogen (erkennungsdienstlicher Bogen) jedoch noch Hinweise auf Vorgänge aus weit zurückliegenden Jahren enthielt, obwohl die entsprechenden Unterlagen zu Recht ausgesondert waren. Der mit der Aussonderung nach den Richtlinien über Kriminalpolizeiliche Sammlungen verfolgte Zweck wird nicht erreicht, wenn die Kriminalakten nach Vernichtung einzelner Unterlagen an anderer Stelle Hinweise auf eben diese ausgesonderten Vorgänge enthalten. Auf meinen diesbezüglichen Hinweis hat das Bayerische Landeskriminalamt auch den ed-Bogen entsprechend den Richtlinien über Kriminalpolizeiliche Sammlungen bereinigt.

3.2.5 Datenübermittlung durch die Polizei

Die Eingabe eines Bürgers, der sich beklagt hatte, daß von einer Polizeibehörde über lange Jahre zurückliegende Vorgänge einer ausländischen Polizeibehörde Mitteilung gemacht worden sei, hat zu einer Reihe von interessanten Fragen geführt:

- a) Die Zulässigkeit einer Datenübermittlung an eine ausländische Behörde beurteilt sich nach Art. 18 Abs. 1 in Verbindung mit Art. 18 Abs. 3 bzw. nach Art. 18 Abs. 4 BayDSG. Die Erteilung von Auskünften an ausländische Polizeidienststellen kann in begründeten Einzelfällen grundsätzlich zur rechtmäßigen Aufgabenerfüllung deutscher Polizeidienststellen gehören. Derartige Datenübermittlungen durch die Polizei sind nach Art. 18 Abs. 4 BayDSG nur zulässig, wenn das öffentliche Interesse sie erfordert. Dies gilt nicht nur für den Datenaustausch über das Bundeskriminalamt, son-

dern in begründeten Einzelfällen auch auf der unteren Polizeidienstebene an benachbarte ausländische Dienststellen im sogenannten „kleinen Grenzverkehr“.

- b) Die Bezeichnung von Eintragungen auf Karteikarten als „gestrichen“ genügt weder den Aussonderungsanforderungen nach den polizeilichen KS-Richtlinien noch dem datenschutzrechtlichen „Löschungsgebot“.
- c) Wird eine Auskunft von einem Beamten erteilt, der sich an die zugrunde liegende Information erinnert, ohne in Akten oder Karteien nachsehen zu müssen, so fällt dieser Vorgang jedenfalls dann unter die Vorschriften des Bayer. Datenschutzgesetzes, wenn die der Auskunft zugrunde liegende Information auch in einer Datei gespeichert ist. Eine Datenübermittlung „aus einer Datei“ liegt demnach bereits dann vor, wenn zwischen den Angaben in einer Datei und der Übermittlung ein gewisser Zusammenhang besteht. Bei einer Auskunft aus dem Erinnerungsvermögen liegt eine nach dem Datenschutzrecht zu beurteilende Datenübermittlung dann vor, wenn die gleichen Daten zur Zeit der Auskunftserteilung noch in Dateien der auskunftserteilenden Stelle gespeichert sind. Bei einer anderen rechtlichen Wertung dieses Vorgangs wäre der Umgehung der Datenschutzgesetze Tür und Tor geöffnet. Denn im nachhinein läßt sich wohl höchst selten mit Sicherheit feststellen, ob Daten tatsächlich aus Dateien oder aber „aus dem Kopf“ eines Sachbearbeiters übermittelt worden sind.
- d) Werden bei einer Datenübermittlung die in den KS-Richtlinien enthaltenen Regelungen zum Informationsaustausch nicht beachtet, so kann aus dieser Verletzung der KS-Richtlinien nicht zwingend auf die Unzulässigkeit der Datenweitergabe nach Art. 17 oder Art. 18 BayDSG geschlossen werden. Dies gilt insbesondere dann, wenn die im Einzelfall nicht beachtete Regelung der KS-Richtlinien nicht Datenschutzzwecken dient.
- e) Werden Daten an eine andere Stelle übermittelt, obwohl diese Daten nach den in den KS-Richtlinien festgelegten Fristen hätten gelöscht sein müssen, so ist diese Datenübermittlung im Regelfall nicht mehr zur „rechtmäßigen Aufgabenerfüllung erforderlich“. Da bei vielen Polizeibehörden die Kriminalakten noch nicht vollständig entsprechend den KS-Richtlinien ausgesondert worden sind, ist grundsätzlich bei jeder Datenübermittlung zu prüfen, ob die zu übermittelnden Daten nicht zwischenzeitlich hätten gelöscht sein müssen. Eine dennoch vorgenommene Datenübermittlung ist grundsätzlich unzulässig.

3.2.6 Registrierung von Reisenden an der Grenze

In meinem letzten Tätigkeitsbericht habe ich darauf hingewiesen, daß die Bayerische Grenzpolizei Reisende an der Grenze zur CSSR registrierte. Meine diesbezüglichen Ermittlungen ergaben, wie auch der Öffentlichkeit durch Pressemitteilungen bekannt wurde, daß die Bayerische Grenzpolizei seit dem Jahr 1952 an den Grenzübergängen zur CSSR die Perso-

nalien von Reisenden im Alter von 16 bis 60 Jahren karteienmäßig erfaßt und im Regelfall 5 Jahre aufbewahrt hat. Wurde innerhalb dieser Frist kein weiterer Grenzübertritt derselben Person festgestellt, so wurde die entsprechende Karteikarte vernichtet. Auskünfte aus diesen dezentralen Karteien wurden mit Sicherheitsaufgaben betrauten Stellen des Bundes und den Strafverfolgungsbehörden erteilt.

Bei Einrichtung dieser Karteien stand die Auskunftserteilung über den Verbleib von Reisenden in der CSSR im Vordergrund. Damals gingen bei der Grenzpolizei zahlreiche Anfragen über vermißte Personen ein, von denen zu vermuten war, daß sie in ein Land des Ostblocks gereist waren. In den letzten Jahren diente die Kartei zunehmend als Hilfsmittel für die Wahrnehmung polizeilicher Aufgaben der Verbrechensbekämpfung (Verschiebung von Kraftfahrzeugen, Rauschgiftschmuggel, Waffenhandel, internationale Kunstdiebstähle). Die Datenerfassung an der Grenze zur CSSR wurde im Berichtsjahr begrenzt, insbesondere wurden Reisegruppen, Pendler, Reisende mit Dienst- oder Diplomatenpaß und Teilnehmer von Betriebsausflügen nicht mehr erfaßt. Die Fragen der umfassenden Datenerhebung und der Datenweitergabe werden derzeit im Zusammenhang mit der Amtshilfeproblematik diskutiert.

3.2.7 Datenabgleich zwischen Kraftfahrzeugzulassungsstellen und der Polizei

In einigen Bundesländern (Niedersachsen, Schleswig-Holstein) wurde erwogen, eine Ausnahme von den Vorschriften des § 26 Abs. 1 Satz 3 und Abs. 5 der Straßenverkehrszulassungsordnung insoweit zuzulassen, als die für das Kraftfahrt-Bundesamt bestimmten Durchschriften der Karteikarten der Zulassungsstellen zunächst der Polizei zum Abgleich mit dem INPOL-System zugeleitet werden. Dem lag die Erkenntnis der Polizei zugrunde, daß die Unterlagen der Zulassungsstellen aktueller als die der Meldebehörden sind.

Auf entsprechende Anfrage hat mir das Bayer. Staatsministerium des Innern mitgeteilt, daß ein derartiger Datenabgleich in Bayern nicht bekannt und derzeit nicht beabsichtigt sei.

Gegen einen derartigen globalen Datenabgleich hätte ich auch nachhaltige Bedenken. Da § 26 Abs. 5 Satz 3 StVZO lediglich Auskünfte im Einzelfall zuläßt und § 70 StVZO nur die Genehmigung von Ausnahmen hinsichtlich der in der Straßenverkehrszulassungsordnung enthaltenen Zulassungsvoraussetzungen vorsieht, wäre eine derartige Datenübermittlung nach Art. 17 Bayer. Datenschutzgesetz zu beurteilen. Eine generelle Übermittlung sämtlicher Durchschriften der für das Kraftfahrt-Bundesamt bestimmten Karteikarten an die Polizei dürfte jedoch nicht generell zur Erfüllung öffentlicher Aufgaben der Polizei erforderlich sein.

3.2.8 Datenerhebung durch ein Abschleppunternehmen im Auftrag der Polizei

Ein privates Abschleppunternehmen hat im Auftrag eines Polizeipräsidiums Kraftfahrzeuge abgeschleppt und verwahrt. Bei Abholung des verwahrten Fahrzeuges

wurden die Abholer danach gefragt, ob sie das betreffende Kraftfahrzeug zur Tatzeit selbst gefahren haben. Diese Aussage wurde auf einer Karteikarte vermerkt, die später an das Polizeipräsidium weitergegeben worden ist.

Ein solches Verfahren halte ich für datenschutzrechtlich bedenklich. Wenngleich die Frage, ob der Abholer zur Tatzeit das Fahrzeug geführt hat, in erster Linie zur Feststellung des Kostenschuldners für den Ersatz der polizeilichen Aufwendungen und zur Rechnungsstellung durch das Polizeipräsidium dienen mag, so diente in der Praxis die Erforschung dieses Sachverhalts auch für ein eventuelles Ordnungswidrigkeiten- oder Strafverfahren. Tatsächlich wurden die Feststellungen nach dem „Fahrzeugführer zur Tatzeit“ im Einzelfall auch bei Gerichten und in Verwaltungsverfahren verwertet, wobei Angehörige des Abschleppunternehmens als Zeugen auftraten. Wäre eine derartige Befragung unmittelbar durch Polizeibeamte vorgenommen worden, so hätten diese die Abholer nach § 163 a Abs. 4 Satz 2 in Verbindung mit § 136 Abs. 1 Satz 2 StPO bzw. nach § 55 OWiG darauf hinweisen müssen, daß es ihnen nach dem Gesetz freistehe, sich zu der Beschuldigung zu äußern oder nicht zur Sache auszusagen.

Abgesehen davon erscheint der Auftrag durch eine Polizeibehörde an ein privates Abschleppunternehmen problematisch, derartige Daten zu erfassen und zu speichern. Nach Nr. 3.3. der Gemeinsamen Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz sollen öffentliche Stellen im Regelfall Aufträge zur Datenverarbeitung an Private nur dann vergeben, wenn die Daten nicht sensibler Art sind. Dies gilt auch, wenn lediglich Aufträge zur Datenerfassung zu vergeben sind. Da bei der Frage nach dem „Führer des Kraftfahrzeugs zur Tatzeit“ möglicherweise Angaben zu Ordnungswidrigkeiten oder strafbaren Handlungen erhoben werden, dürfte eine derartige Beauftragung eines Privatunternehmens insoweit generell unzulässig sein.

Auf diese Bedenken hin hat das Polizeipräsidium zunächst verfügt, daß der Abholer vor der Beantwortung der Frage nach dem Führer des Kraftfahrzeugs zur Tatzeit darauf aufmerksam zu machen sei, daß diese Angaben ausschließlich wegen der noch zu erstellenden Kostenrechnung und damit zur Feststellung des Kostenschuldners notwendig seien. Im übrigen war verfügt worden, daß diese Information nur noch an die Kostenstelle weitergegeben werden dürfe und eine weitere Verwendung dieser Information, insbesondere im Hinblick auf ein Straf- oder Ordnungswidrigkeitenverfahren ausgeschlossen sei. Inzwischen hat das Polizeipräsidium das Abschleppunternehmen angewiesen, die Frage nach dem „Kraftfahrzeugführer zur Tatzeit“ nicht mehr zu stellen. Das Bayer. Staatsministerium des Innern hat auf meine Anregung hin die übrigen Polizeipräsidien gebeten, ebenfalls auf die Feststellung des Fahrers zur Tatzeit bei den privaten Verwahrstellen zu verzichten.

3.2.9 Fragebogen zur Beurteilung der Glaubwürdigkeit kindlicher Zeugen

Der Berliner Datenschutzbeauftragte hat mir mitgeteilt, daß der dortige Polizeipräsident im Rahmen von

Ermittlungsverfahren, bei denen Schüler als Zeugen beteiligt sind, an die Schulen herantrete und die jeweiligen Schulleitungen bitte, vom Klassen- oder Fachlehrer bei Schülern beobachtete Auffälligkeiten zu einzelnen Fragenkomplexen mitzuteilen. Diese Fragen berühren teilweise sehr sensible Bereiche. So sollen Auskünfte über die geistige Entwicklung, den körperlichen Entwicklungsstand, längere Krankheiten, Auffälligkeiten des Schülers in sexueller Hinsicht, aber auch über dessen häusliche Verhältnisse gegeben werden.

Meine Ermittlungen nach der diesbezüglichen bayerischen Praxis haben bisher folgendes ergeben: In Bayern war in einer Bekanntmachung vom 4. Januar 1956 über die Behandlung von Kindern und Jugendlichen bei der Polizei bestimmt, daß die bei der Vernehmung von Kindern und Jugendlichen gemachten Beobachtungen, wie beispielsweise deren körperliche Entwicklung, geistige Reife, persönliches Verhalten während der Vernehmung in einem Aktenvermerk niederzulegen, gegebenenfalls durch die Einholung eines schriftlichen Schulgutachtens zu ergänzen seien. Ersuchen um Überlassung des Schülerbogens oder um Übermittlung einer Auskunft aus ihm sollten an das zuständige Bezirks- oder Stadtschulamt gerichtet werden. Auf Grund dieser Bekanntmachung haben Polizeidienststellen in Fällen, in denen dies zur Förderung der strafrechtlichen Ermittlungen notwendig schien, die Schulleitungen durch Übersendung eines Fragebogens um entsprechende Auskünfte gebeten. Die vorgenannte Bekanntmachung ist zwischenzeitlich durch eine Polizeidienstvorschrift „Bearbeitung von Jugendsachen bei der Polizei“ abgelöst worden. Diese Dienstvorschrift sieht die Einholung von derartigen Schulgutachten nicht mehr vor, wenngleich die Erholung solcher Schulgutachten darin auch nicht untersagt wird. Offensichtlich haben einzelne Polizeidienststellen in den letzten Jahren selbst entwickelte Fragebögen an Schulleitungen im Zusammenhang mit Ermittlungsverfahren versandt. Eine abschließende Information über den Umfang und den Inhalt derartiger Fragebögen liegt mir noch nicht vor. Ich werde die Angelegenheit weiter verfolgen.

3.2.10 Gutachtenverwaltung im Bayer. Landes-kriminalamt

Das Bayerische Landeskriminalamt erstattet im Auftrag von Gerichten, Staatsanwaltschaften und Polizeibehörden jährlich mehrere tausend Gutachten. Eingang und Erledigung dieser Gutachtenaufträge wurden bislang in einem entsprechenden Tagebuch vermerkt. Nun hat das Landeskriminalamt zur Verwaltung der Gutachtensaufträge ein EDV-Verfahren entwickelt, das zwischenzeitlich vom Bayer. Staatsministerium des Innern auch freigegeben worden ist: In diesem EDV-Verfahren werden neben anderen Daten jedenfalls auch die Personalien der Personen gespeichert, die im Betreff eines an das Landeskriminalamt gerichteten Gutachtenssuchens aufgeführt sind. Dies erscheint mir nicht unbedenklich, zumal hierbei auch Name, Vorname und Geburtsdatum eines Geschädigten und eines sonst in Zusammenhang mit einer Straftat Beteiligten erfaßt werden können. Zur Erstellung von Gutachten durch das Landes-

kriminalamt dürfte diese Speicherung der Personalien weder für die Überwachung der fristgerechten Gutachtenerstellung noch für eventuelle Rückfragen des Gutachtauftraggebers zwingend erforderlich sein, weil hierfür eindeutiger Daten wie Aktenzeichen und Fernschreibnummern des Absenders zur Verfügung stehen.

Das Bayer. Staatsministerium des Innern hat mir versichert, daß diese Daten zur Gutachtenverwaltung gesondert von den übrigen polizeilichen Dateien geführt würden und ein Zugriff durch die sachbearbeitenden Polizeidienststellen grundsätzlich nicht möglich sei. Dennoch ist es meines Erachtens nicht ausgeschlossen, daß auch diese Daten in Einzelfällen losgelöst von den Zwecken der Gutachtenverwaltung für polizeiliche Ermittlungszwecke durchgesehen und ausgewertet werden. Hierin liegt ein wenn auch geringes Risiko, daß Zeugen oder sonstige Beteiligte eines Strafverfahrens in einem anderen Ermittlungsverfahren ohne weiteres Zutun zu Verdächtigen werden können. Gerade solchen Risiken gilt es jedoch mit dem Datenschutz entgegenzuwirken.

3.2.11 Verfassungsschutz

3.2.11.1 Ergebnis bisheriger Überprüfungen

Beim Bayerischen Landesamt für Verfassungsschutz habe ich im Berichtszeitraum auf Grund von Bürgeranfragen eine Reihe von Einzelüberprüfungen vorgenommen. In keinem dieser Fälle hat sich ein Anlaß zu einer Beanstandung wegen Verletzung datenschutzrechtlicher Vorschriften ergeben. Die von mir verlangte Einsicht in Dateien und Unterlagen wurde mir in allen Fällen gewährt. Eine Berufung auf Art. 28 Abs. 3 Satz 2 Bayerisches Datenschutzgesetz, wonach die Einsicht in Unterlagen und Akten verweigert werden kann, wenn dies die Sicherheit des Bundes oder eines Landes gefährden würde, erfolgte nicht.

3.2.11.2 Mitteilungen über das Prüfungsergebnis

Der dem Bürger nach Art. 8 Abs. 1 BayDSG eingeräumte Anspruch, auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu verlangen, besteht nach Art. 8 Abs. 2 Nr. 5 Bayerisches Datenschutzgesetz nicht gegenüber Verfassungsschutzbehörden. Zwar ist der Landesbeauftragte für den Datenschutz an die letztgenannte Bestimmung nicht gebunden, dennoch hielte ich es, wie bereits in meinem letzten Tätigkeitsbericht ausgeführt, für eine unzulässige Umgehung des Gesetzes, wenn der Bürger über das Prüfungsergebnis bei Verfassungsschutzbehörden im Detail unterrichtet würde. Im übrigen darf sich der Landesbeauftragte für den Datenschutz nicht dem Risiko aussetzen, als möglicher Ansatzpunkt für Ausforschungen zu gelten.

Deshalb teile ich in derartigen Fällen grundsätzlich nur mit, daß die erbetene Überprüfung bei den Verfassungsschutzbehörden vorgenommen worden ist. Ich bin mir bewußt, daß diese Sachbehandlung nicht immer befriedigend ist. Manche Bürger fühlen sich durch eine derartige Mitteilung unbegründet in ihrem Verdacht bestärkt, daß beim Landesamt für Verfassungsschutz Daten über sie gespeichert würden.

Trotz dieser unbefriedigenden Situation kann ich von dieser Verfahrensweise nur dann abgehen, wenn das Landesamt für Verfassungsschutz selbst keine Gefahr der Ausforschung sieht und seinerseits dem Bürger über die Tatsache Mitteilung gibt, ob zu seiner Person Daten gespeichert sind oder nicht.

3.2.11.3 Weitergabe von Daten des Verfassungsschutzes an ausländische Geheimdienste

Durch Presseveröffentlichungen ist auch einer breiteren Öffentlichkeit bekannt geworden, daß deutsche Verfassungsschutzbehörden im Einzelfall Daten über deutsche Staatsbürger an ausländische Behörden übermitteln. Rechtsgrundlage für eine Zusammenarbeit des Bayerischen Landesamts für Verfassungsschutz mit ausländischen Behörden ist insbesondere Art. 3 des Zusatzabkommens zum Nato-Truppen-Statut (BGBl. 1961 II Seite 1218, ratifiziert durch Gesetz vom 8. August 1961, BGBl. II Seite 1183). Dieses Abkommen gilt jedoch nur für die Zusammenarbeit mit Behörden der Nato-Truppen. Eine über die vorgenannte Rechtsgrundlage hinausgehende Zusammenarbeit, für die ich bislang keine Anhaltspunkte gewonnen habe, müßte an den tragenden Grundsätzen der Verfassung und dem Bayerischen Datenschutzgesetz gemessen werden.

3.3 Justiz

Die Vorschriften des Bayerischen Datenschutzgesetzes gelten grundsätzlich auch für den Geschäftsbereich des Bayerischen Staatsministeriums der Justiz. Die Verarbeitung personenbezogener Daten in Dateien ist jedoch in diesem Geschäftsbereich vergleichsweise gering, so daß das Bayerische Datenschutzgesetz unmittelbar nur in verhältnismäßig bescheidenem Umfang Anwendung findet. Allerdings besteht, wie bei allen Verwaltungen, auch bei der Justiz kein datenschutzfreier Raum. Denn soweit die Speicherung und Übermittlung von Daten durch Gerichte und Staatsanwaltschaften nicht spezialgesetzlich geregelt ist, muß grundsätzlich auf die tragenden Bestimmungen der Verfassung zum Schutz der Persönlichkeit zurückgegriffen werden.

Das Grundgesetz gewährt, wie das Bundesverfassungsgericht in ständiger Rechtsprechung anerkannt hat, dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung, der jeder Einwirkung der öffentlichen Gewalt entzogen ist. Grundlage des Gebots, die Intimsphäre des einzelnen zu achten, ist das durch Art. 2 Abs. 1 Grundgesetz verbürgte Recht auf freie Entfaltung der Persönlichkeit. Weiterhin ist bei der Bestimmung von Inhalt und Tragweite dieses Grundrechts zu berücksichtigen, daß nach Art. 1 Abs. 1 Grundgesetz die Würde des Menschen unantastbar ist und gegenüber aller staatlichen Gewalt Achtung und Schutz beansprucht. Allerdings fällt nicht etwa der gesamte Persönlichkeitsbereich unter den Schutz der Art. 1 Abs. 1, 2 Abs. 1, 19 Abs. 2 Grundgesetz. Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger muß jedermann die Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebotes erfolgen, soweit sie nicht den un-

antastbaren Bereich privater Lebensgestaltung beeinträchtigen.

Die personenbezogenen Daten, die der Justiz über den einzelnen bekannt werden, sind jedoch grundsätzlich nicht ausnahmslos dem schlechthin unantastbaren Bereich privater Lebensgestaltung zuzuordnen, der nach der Rechtsprechung des Bundesverfassungsgerichts jedem Zugriff der öffentlichen Gewalt von vorneherein verschlossen ist. Die von der Tätigkeit der Justizbehörden berührten Lebenssachverhalte haben in aller Regel einen Bezug zu anderen Personen, wodurch der innerste Bezirk verlassen wird, der dem einzelnen um seiner selbstverantwortlichen Persönlichkeitsentfaltung willen verbleiben muß. Dennoch setzt das Grundrecht des Bürgers auf Achtung seiner Privatsphäre Gerichten und Staatsanwaltschaften bei der Verarbeitung von Daten auch dort Schranken, wo der einzelne in Beziehungen zu Mitmenschen getreten ist. Die hierbei erforderliche Güter- und Interessenabwägung ist nun durch die Datenschutzgesetze näher konkretisiert. Somit bestehen generell keine Bedenken, die entsprechenden Bestimmungen des Bayerischen Datenschutzgesetzes als Entscheidungshilfe mit heranzuziehen, wenn es gilt, die Zulässigkeit der Speicherung oder Übermittlung personenbezogener Daten durch Gerichte und Staatsanwaltschaften zu beurteilen. Es kann deshalb auch für den nicht unter den Schutz des Bayerischen Datenschutzgesetzes fallenden Bereich grundsätzlich davon ausgegangen werden, daß die Speicherung und Übermittlung personenbezogener Daten nur zulässig ist, wenn sie zur rechtmäßigen Erfüllung einer öffentlichen Aufgabe der öffentlichen Stelle erforderlich ist oder — bei der Übermittlung — der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

3.3.1 Mitteilungen in Strafsachen (MiStra)

Nach der Anordnung über Mitteilungen in Strafsachen (MiStra) unterrichten Gerichte und Staatsanwaltschaften andere Behörden und Stellen über Entscheidungen in Strafsachen. Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz haben sich mit der Frage der Rechtmäßigkeit der nach der MiStra vorgenommenen Datenübermittlungen auseinandergesetzt. In einem hierzu ergangenen Beschluß haben die Datenschutzbeauftragten festgestellt, daß die MiStra wichtigen Grundentscheidungen des Gesetzgebers und des Bundesverfassungsgerichts nicht mehr entspricht. Die Datenschutzgesetze des Bundes und der Länder haben die Verarbeitung personenbezogener Daten rechtlichen Beschränkungen unterworfen. Bereichsspezifische Gesetze wie das Bundeszentralregistergesetz, das Bundespersonalausweisgesetz, das Melderechtsrahmengesetz sowie mehrere einschlägige Entscheidungen des Bundesverfassungsgerichts sind Belege dafür, daß der Staat in vielen Fällen bewußt davon absieht, die verfügbaren Informationen allen daran möglicherweise interessierten Stellen zur Kenntnis zu geben. Demgegenüber ist die MiStra von der gegenteiligen Auffassung geprägt. Noch werden Strafurteile nebst den Gründen in einem

weitgehend formalisierten Verfahren weit gestreut. Nur in vergleichsweise wenigen Fällen werden jedoch durch die Mitteilungen auf Grund gesetzlicher Vorschriften Maßnahmen (z. B. dienstrechtlicher oder disziplinarischer Art) ausgelöst. Diese Maßnahmen sind grundsätzlich gerichtlich nachprüfbar. In einer Vielzahl von Fällen werden die Mitteilungen aber zunächst nur zu den Akten genommen. Erst später können sie bei den dann anstehenden Entscheidungen nachteilige Wirkungen entfalten, ohne daß dies jedoch immer meßbar und nachprüfbar wäre. So läßt sich generell feststellen, daß die Anwendung der MiStra vielfach zu einer globalen und schematischen Übermittlung besonders sensibler Daten führt, die im Regelfall eine Einzelfallprüfung unter Beachtung des Grundsatzes der Verhältnismäßigkeit vermissen läßt. Da Mitteilungen dieser Art in die nach Art. 2 Abs. 1 des Grundgesetzes geschützte Rechtssphäre des Betroffenen eingreifen können, bedürfen sie grundsätzlich einer gesetzlichen Grundlage.

Ich habe daher das Bayerische Staatsministerium der Justiz gebeten, die MiStra auf ihre Rechts-, insbesondere Verfassungsmäßigkeit zu überprüfen, neuere Tendenzen des Datenschutzrechts zu berücksichtigen, die MiStra insgesamt möglichst eindeutig zu fassen und im übrigen die Rechtsgrundlagen für die Mitteilungspflichten im einzelnen zu bezeichnen.

3.3.2 Zentraldateien der Staatsanwaltschaften

Die Staatsanwaltschaften führen zur Erledigung ihrer Aufgaben Strafakten. Zum gezielten Zugriff auf einzelne Akten sind bei den Staatsanwaltschaften zentrale Namenverzeichnisse, genannt „Zentrale Namenskartei“ eingerichtet. In Bayern sind die zentralen Namenskarteien durch § 47 Abs. 4 Satz 2 Aktenordnung vorgesehen. Sie dienen der Führung des zentralen Aktenregisters und des Namenverzeichnisses zu dem Aktenregister und werden grundsätzlich in Kartei- oder in Buchform geführt. Nur den Staatsanwaltschaften bei den Landgerichten München I und Nürnberg steht hierzu ein automatisiertes Verfahren zur Verfügung. In diesen Namenskarteien werden die Namen der Beschuldigten und der Betroffenen gespeichert. Außerdem werden die zur Last gelegte Straftat sowie teilweise der Ausgang des Verfahrens vermerkt.

Eine von den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz eingesetzte Arbeitsgruppe prüft unter bayerischer Federführung derzeit, wie aus datenschutzrechtlicher Sicht derartige zentrale Namenskarteien der Staatsanwaltschaften zu beurteilen sind.

3.3.3 Prozeßkostenhilfe

Das am 1. Januar 1981 in Kraft getretene Gesetz über die Prozeßkostenhilfe hat die bisherigen Vorschriften in der Zivilprozeßordnung zum Armenrecht abgelöst. Wer Prozeßkostenhilfe beantragt, muß eine Erklärung abgeben über seine persönlichen und wirtschaftlichen Verhältnisse, insbesondere Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten, sowie dem Antrag entsprechende Belege beifügen. Wegen der

möglichen Sensibilität dieser Angaben kann der Antragsteller ein erhebliches Interesse daran haben, daß seine Angaben anderen Personen möglichst nicht bekannt werden.

Um diesem Anliegen Rechnung zu tragen, habe ich eine entsprechende Anregung des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen aufgegriffen und das Bayer. Staatsministerium der Justiz gebeten, die im Rahmen des Verfahrens zur Gewährung der Prozeßkostenhilfe angefallenen Belege in einer Beiakte zu führen. Bei dieser Anregung bin ich davon ausgegangen, daß zwar dem Antragsgegner im Zivilrechtsstreit die Einsicht in die Unterlagen über die Vermögensverhältnisse des Antragstellers grundsätzlich nicht vollständig verwehrt werden kann, dritten Personen diese Unterlagen im Rahmen der ihnen eventuell nach § 299 Zivilprozeßordnung (ZPO) zu gewährenden Akteneinsicht regelmäßig nicht zugänglich sein müssen. Eine zwangsläufige Kenntnisnahme der Unterlagen zur Gewährung der Prozeßkostenhilfe durch Dritte bei jeder Akteneinsicht wird durch eine getrennte Aktenführung verhindert. Im übrigen erinnert eine gesonderte Führung der für die Bewilligung der Prozeßkostenhilfe notwendigen Unterlagen in einer Beiakte den Vorstand des Gerichts bei seiner Entscheidung nach § 299 Abs. 2 ZPO daran, daß auch hinsichtlich dieser Erklärungen und Belege das rechtliche Interesse an der Akteneinsicht selbständig zu prüfen ist.

Diesem Anliegen haben die Landesjustizverwaltungen weitgehend Rechnung getragen. In den am 10. Dezember 1980 bundeseinheitlich erlassenen Durchführungsbestimmungen zum Gesetz über die Prozeßkostenhilfe wurde unter Nr. 2.2 folgende Bestimmung aufgenommen:

„Der Vorgang mit der Erklärung über die persönlichen und wirtschaftlichen Verhältnisse sowie die bei der Durchführung der Prozeßkostenhilfe entstehenden Vorgänge sind in einem Beiheft zu vereinigen. Dies gilt insbesondere für Kostenrechnungen, Beanstandungen, Zahlungsanzeigen und Nachrichten. Zu dem Beiheft sind ferner Durchschriften der die Prozeßkostenhilfe betreffenden gerichtlichen Entscheidungen zu nehmen.“

Erfreulicherweise ist in der für Bayern geltenden Fassung noch zusätzlich folgende Bestimmung aufgenommen worden:

„Bei Versendung der Akten ist das Beiheft zurückzubehalten.“

3.3.4 Benachrichtigung des Finanzamtes über die Entschädigung für Strafverfolgungsmaßnahmen

Erhält ein Bürger nach dem Gesetz über die Entschädigung für Strafverfolgungsmaßnahmen (StrEG) eine Entschädigung aus der Staatskasse, so ist das für den Wohnsitz des Zahlungsempfängers zuständige Finanzamt von der Zahlung der Entschädigung zu benachrichtigen. Inhalt und Form dieser Benachrichtigungen des zuständigen Finanzamtes sind bei den einzelnen Staatsanwaltschaften in Bayern unterschiedlich. Während derartige Mitteilungen teilweise

nur auf wenige Angaben beschränkt sind, wird in anderen Fällen das Finanzamt durch Übersendung eines vollständigen Abdruckes der getroffenen Entscheidung über die gezahlte Entschädigung benachrichtigt. Bei der letztgenannten Sachbehandlung können dem Finanzamt neben den für eine etwaige Besteuerung erforderlichen Daten noch weitere Tatsachen über die Strafverfolgung bekannt werden, die das Finanzamt zu seiner Aufgabenerledigung nicht benötigt.

Da eine Datenübermittlung nach § 111 Abs. 1 Satz 1 AO, dem Art. 17 Abs. 1 BayDSG entspricht, nur zulässig ist, wenn sie zur rechtmäßigen Aufgabenerfüllung „erforderlich“ ist, und im übrigen die Bestimmung des Art. 17 BayDSG bei der Prüfung des erforderlichen Umfangs der Datenübermittlung in der vorstehenden Angelegenheit zumindest als Entscheidungshilfe mit heranzuziehen ist, sollte die bei der Benachrichtigung des Finanzamtes vorgenommene Datenübermittlung auf das erforderliche Maß beschränkt werden.

Bei dieser Prüfung ist auch zu berücksichtigen, daß die Zahlung von derartigen Entschädigungen insbesondere auf dem Gebiet der Ertragssteuern von Bedeutung sein kann. Ob die einzelne Entschädigungszahlung steuerlich relevant ist oder nicht, hängt insbesondere von der Art des Schadens ab, der durch die Zahlung ausgeglichen werden soll. Während der Ausgleich von Nichtvermögensschäden regelmäßig keine steuerlichen Auswirkungen haben wird, ist aber der Ersatz eines entgangenen Gewinns grundsätzlich beachtlich. Unter Berücksichtigung der Erfordernisse der Finanzämter wird daher eine Mitteilung, die sich nur auf die Höhe des auszahlenden Betrags und die Tatsache beschränkt, daß die Zahlung der Entschädigung für Strafverfolgungsmaßnahmen geeignet hat, nicht ausreichend sein. Für diese Datenübermittlung im Einzelfall dürften zur Benachrichtigung des Finanzamtes allenfalls folgende Angaben erforderlich sein:

- Name und Adresse des Zahlungsempfängers
- Höhe der Entschädigung
- Angabe, für welche Art von Schäden der Ausgleich gewährt werden soll
- Tag der Auszahlung (bedeutsam für die zeitliche Zuordnung).

Entbehrlich sind in diesem Zusammenhang jedoch insbesondere Angaben über den Entschädigungsgrund und die Strafverfolgungsmaßnahmen im einzelnen. Gerade diese Angaben könnten aber für den betroffenen Personenkreis unnötig belastend wirken, weil die Betroffenen von dem ihnen zunächst zur Last gelegten Strafvorwurf entlastet worden sind.

Ich habe das Bayer. Staatsministerium der Justiz gebeten, künftig von der Übersendung eines Abdruckes der vollständigen Entscheidung abzusehen und die Mitteilung auf die vorgenannten Angaben zu beschränken. Dieser Bitte hat das Bayer. Staatsministerium der Justiz zwischenzeitlich durch eine entsprechende Weisung an die Staatsanwaltschaften entsprochen, wonach in solchen Fällen den Finanzbehörden lediglich Name und Anschrift des Zahlungs-

empfängers, die Höhe der Entschädigung und der Tag der Auszahlung mitzuteilen sind.

3.3.5 Schuldnerverzeichnis

Nach § 915 Zivilprozeßordnung führt das Amtsgericht – Vollstreckungsgericht ein Verzeichnis der Personen, die vor diesem Gericht die eidesstattliche Versicherung über ihre Vermögensverhältnisse abgelegt haben oder gegen die wegen Nichtabgabe dieser eidesstattlichen Versicherung Haft angeordnet worden ist. Die Eintragungen im Schuldnerverzeichnis werden nach Ablauf einer bestimmten Frist gelöscht.

Weil eine nicht unerhebliche Zahl von Institutionen und Personen Abschriften aus dem Schuldnerverzeichnis erhalten, ist die Beachtung dieser Lösungsfrist bei den Empfängern der Abschriften in der Praxis vielfach nicht gewährleistet. Die bisherige Handhabung der Verteilung von Abschriften aus dem Schuldnerverzeichnis bedarf dringend einer Änderung. Auf entsprechende Anregungen der Datenschutzbeauftragten des Bundes und der Länder hat der Bundesminister der Justiz einen Entwurf einer Verordnung über Abschriften aus dem Schuldnerverzeichnis erarbeitet und den Landesjustizverwaltungen zur Stellungnahme zugeleitet. Mit diesem Entwurf ist beabsichtigt, den Kreis derjenigen Stellen einzuengen, der derzeit Schuldnerlisten beziehen darf. Zudem soll die Verwertungsbefugnis der sogenannten „Zweitempfänger“ eingeschränkt werden, die über die vorgenannten Stellen weitere Abschriften der Schuldnerverzeichnisse oder Auskünfte daraus erhalten haben.

Aus der Sicht des Datenschutzes begrüße ich den vorliegenden Entwurf, weil er gegenüber der derzeit geltenden Regelung Verbesserungen enthält. Er bedarf jedoch noch einiger Änderungen, weil er m. E. dem Anliegen des Datenschutzes nicht in allen Punkten gerecht wird.

3.4 Sozial- und Gesundheitsbereich

3.4.1 Besondere Vorschriften über den Datenschutz im 10. Buch des Sozialgesetzbuches (SGB X)

Die §§ 67 ff. SGB X (BGBl. I 1980, S. 1484 ff.), die seit 1. 1. 1981 in Kraft sind, enthalten besondere Vorschriften über den Datenschutz für die in § 35 SGB I aufgeführten Sozialleistungsträger (Neufassung des § 35: siehe BGBl. I 1980 S. 1499). Neben den reinen Sozialleistungsträgern, wie Landesversicherungsanstalten, Ortskrankenkassen und Berufsgenossenschaften, sind hiervon auch Gemeinden, Landkreise und Bezirke als Sozialleistungsträger, z. B. beim Vollzug der Ausbildungsförderung, des Bundesversorgungsgesetzes, des Wohngeldgesetzes, des Jugendwohlfahrtsgesetzes, des Bundessozialhilfegesetzes und des Bundeskindergeldgesetzes betroffen. Bei Gemeinden müssen also z. B. Jugendamt, Sozialamt, Amt für Ausbildungsförderung, Gesundheitsamt diese Vorschriften beachten. Die neuen Datenschutzregelungen sind für eine Vielzahl öffentlicher Stellen in Bayern von Bedeutung. Bei der Anwendung des neuen Rechts sind bereits einige verfahrensmäßige sowie grundsätzliche Fragen sowie eine Vielzahl von

Einzelfragen bekannt geworden. Im folgenden wird aus der Sicht des Datenschutzes kurz auf wichtige Verfahrensfragen eingegangen:

Meldung zum Datenschutzregister

§ 79 Abs. 1 SGB X erklärt die materiellen Vorschriften des BDSG, also Bundesrecht für anwendbar. § 79 Abs. 3 SGB X sieht aber vor, daß anstelle des Bundesbeauftragten für den Datenschutz die nach Landesrecht zuständigen Stellen treten. Die Kontrolle des Datenschutzes durch den Landesbeauftragten für den Datenschutz bleibt durch die Vorschriften des SGB also unberührt. Nach der Ansicht der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz sowie der Datenschutzkommission Rheinland-Pfalz verbleibt es deshalb bei dem im jeweiligen Landesdatenschutzrecht vorgesehenen Umfang und Verfahren der Datenschutzkontrolle und damit auch bei der landesrechtlichen Regelung der Meldung zum Datenschutzregister. Es wäre nicht einzusehen, daß gerade im sensiblen Datenbereich der Sozialleistungsträger die durch das Datenschutzregister zu schaffende Transparenz geringer sein sollte, als hinsichtlich der Datenspeicherung anderer öffentlicher Stellen. Dies wäre jedoch der Fall, wenn anstatt der Landes-Datenschutz-Registervorschrift nur die stark verkürzte Meldung nach der Bundes-Datenschutz-Registerordnung abzugeben wäre. Außerdem müßten dann z. B. Gemeinden und Landratsämter je nach Aufgabe unterschiedliche Meldeformulare benutzen, was zu unnötigem Verwaltungsaufwand und mit Sicherheit auch zu Fehlern in der Meldung führen würde. Überdies haben die meisten bayerischen Sozialleistungsträger ihre automatisierten Dateien bereits nach dem bayerischen Landesrecht zum Bayer. Datenschutzregister gemeldet.

Verpflichtung auf das Datengeheimnis

Die aufgrund § 79 Abs. 2 SGB X für die Verpflichtung auf das Datengeheimnis maßgebliche Vorschrift des § 5 BDSG sieht die Verpflichtung auch solcher Personen vor, die nicht bei der automatisierten, sondern bei der herkömmlichen Datenverarbeitung (z. B. mit Hilfe von Karteien) beschäftigt sind. Dieser Personenkreis mußte unverzüglich nachverpflichtet werden. Soweit nach dem bis Ende 1980 für Sozialleistungsträger geltenden bayerischen Datenschutzrecht Verpflichtungen auf das Datengeheimnis im Zusammenhang mit automatisierter Datenverarbeitung vorgenommen wurden, müssen die Verpflichteten m. E. noch auf die neuen Datenschutzvorschriften des SGB X (§§ 67 ff. und 79 ff.) hingewiesen werden.

Bestellung von internen Datenschutzbeauftragten

Nach § 79 Abs. 1 SGB X sind bei öffentlichen Stellen, die unter § 35 Abs. 1 SGB I fallen (siehe oben), §§ 28 und 29 BDSG entsprechend anzuwenden. § 28 BDSG sieht die Bestellung eines internen Beauftragten für den Datenschutz vor, wenn „personenbezogene Daten automatisch“ verarbeitet „und hierbei in der Regel mindestens fünf Arbeitnehmer ständig“ beschäftigt werden bzw. wenn solche Daten auf andere Weise verarbeitet werden, und soweit hierbei in der Regel mindestens „zwanzig Arbeitnehmer ständig beschäftigt sind“. § 79 Abs. 1 SGB X sieht die „entsprechen-

de“ Anwendung der genannten BDSG-Vorschriften vor, da diese – für den nichtöffentlichen Bereich formuliert – nicht ohne entsprechende Umsetzung für öffentliche Stellen passen. Die unter Art. 35 SGB I fallenden Stellen (s. o.) sind daher verpflichtet, einen dem „internen Datenschutzbeauftragten“ bei nicht-öffentlichen Stellen entsprechenden „internen Datenschutzbeauftragten“ zu bestellen. Dies gilt auch für Gemeinden und andere Gebietskörperschaften. Nach der Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz (VollzBek zu Art. 26, Nr. 26.1 ff., 26.4) ist für deren sonstigen Aufgaben die Bestellung eines allgemeinen internen Datenschutzbeauftragten empfohlen. Die Aufgaben des internen Datenschutzbeauftragten nach den Bestimmungen des SGB und der Vollzugsbekanntmachung sollten, um eine zweckmäßige Konzentration von Datenschutz-Fachwissen zu erreichen, gemeinsam wahrgenommen werden.

3.4.2 Einsichtnahme in Sozialhilfeunterlagen durch Mitarbeiter einer Hochschule

In einer Eingabe wurde Beschwerde über folgenden Vorgang geführt: Ein Hochschullehrer hatte zum Zwecke wissenschaftlicher Forschung Sozialhilfeempfängern durch eine Stadtverwaltung ein Schreiben übersenden lassen, in dem er um Einwilligung zur Einsichtnahme in die bei der Stadt geführten Sozialhilfeakten bat. In dem Schreiben wurde unter anderem ausgeführt, daß diese Einwilligung nach dem am 1. 1. 1981 in Kraft tretenden Vorschriften des SGB X ohnehin nicht mehr erforderlich sei.

Das Offenbaren von Angaben aus Sozialhilfeakten gegenüber Außenstehenden war zur Zeit dieses Vorfalles gemäß § 35 Abs. 1 Satz 2 SGB I nur dann ohne Zustimmung des Betroffenen zulässig, wenn eine gesetzliche Mitteilungspflicht bestand. Eine solche war nicht gegeben. Auch nach § 75 Abs. 1 SGB X, in Kraft seit 1. 1. 1981, ist eine Offenbarung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung im Sozialleistungsbereich nicht zulässig, soweit es zumutbar ist, die Einwilligung des Betroffenen nach § 67 SGB X einzuholen. Daß die Einholung der Zustimmungen im vorliegenden Fall zumutbar waren, ergab sich daraus, daß die Stadtverwaltung die Einwilligungen einholen konnte und auch tatsächlich einholte. Da aber nicht bekannt war, ob der Hinweis, die Einwilligung sei ab 1. 1. 1981 ohnehin nicht mehr erforderlich, die Angeschriebenen dazu veranlaßt haben könnte, zu unterschreiben, bestand Unklarheit über die Wirksamkeit der Einwilligungen. Ich hatte deshalb vorgeschlagen, in diesen Fällen keine Einsicht in die Sozialhilfeakten zu gewähren, sondern die Akten durch die zuständigen städtischen Bediensteten auswerten und die für das Forschungsprojekt notwendigen Angaben in anonymisierter Form an den Hochschullehrer übergeben zu lassen.

Das Beispiel zeigt, daß bei der Bitte um Offenbarung von Daten zu Forschungszwecken nach § 75 Abs. 1 SGB X jeweils sorgfältig geprüft werden muß, ob es zumutbar ist, die Einwilligung des Betroffenen einzuholen. Es gibt keine Vermutung, die dafür spräche, daß das Einholen der Einwilligung unzumutbar wäre.

Hinsichtlich der Offenbarung medizinischer Daten sei darauf hingewiesen, daß sie durch § 76 Abs. 1 SGB X,

bei fehlender Einwilligung des Betroffenen, auf die Fälle beschränkt wird, in denen der Arzt, von dem die Daten stammen, selbst zur Offenbarung befugt wäre. Der Empfänger von Daten hat überdies die Zweckbindung und die Geheimhaltungspflicht nach § 78 SGB X zu beachten.

3.4.3 Anwendbarkeit des Bundesdatenschutzgesetzes auf Krankenhäuser

Die Krankenhäuser, deren Träger öffentliche Stellen sind, gelten nach der gegenwärtig herrschenden Auffassung i. d. R. als öffentliche Stellen, die am Wettbewerb teilnehmen. Auf sie sind deshalb gemäß Art. 22 BayDSG die Vorschriften des Bundesdatenschutzgesetzes anzuwenden, soweit nicht gem. Art. 2 Abs. 2 BayDSG besondere Vorschriften über den Datenschutz oder Verschwiegenheitspflichten vorgehen (wie z. B. § 203 StGB und Art. 13 Bayer. Krankenhausgesetz). Mit Ausnahme des Art. 26 Abs. 2 BayDSG gelten allerdings die Überwachungsvorschriften des 5. Abschnittes des BayDSG, so daß es bei der Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz verbleibt.

Für Krankenhäuser und Sozialleistungsträger gelten die materiellen Vorschriften des Bundesdatenschutzgesetzes ab 1. 1. 1981 aufgrund § 79 Abs. 2 SGB X (BGBl. I 1980 S. 1469). Nach § 79 Abs. 3 SGB X ist zur Kontrolle des Datenschutzes nach wie vor der Landesbeauftragte für den Datenschutz zuständig.

Die Anwendbarkeit der materiellen Vorschriften des BDSG führt unter anderem dazu, daß das gesamte bei der Datenverarbeitung beschäftigte Personal auf das Datengeheimnis (§ 5 BDSG) zu verpflichten ist. Im Gegensatz zu Art. 14 Abs. 1 BayDSG ist hier auch die nichtautomatisierte Datenverarbeitung (z. B. Karteiführung) einzubeziehen. Für Krankenhäuser von Sozialleistungsträgern gilt ab 1. 1. 1981 die Vorschrift über die Bestellung eines internen Beauftragten für den Datenschutz in §§ 28, 29 BDSG entsprechend (§ 79 Abs. 1 SGB X, s. o.). Bei öffentlichen Krankenhäusern anderer Träger, auf die das BDSG über Art. 22 Abs. 1 BayDSG anzuwenden ist, bleibt es bei der allgemeinen Regelung der Bayer. Vollzugsbekanntmachung zu Art. 26 BayDSG.

Zu Datensicherungsmaßnahmen bei Krankenhäusern siehe Nr. 3.11.2.

3.4.4 Übermittlung von Patientendaten durch Krankenhäuser zu Werbezwecken

Hersteller von Baby-Artikeln treten immer wieder an Krankenhäuser heran, um die Adressen der Mütter von Neugeborenen zu erfahren. Einer solchen Offenbarung steht der Grundsatz der ärztlichen Schweigepflicht und die Vorschrift des Art. 13 Abs. 5 des Bayer. Krankenhausgesetzes (GVBl. 1974 S. 256) entgegen. Die genannten Vorschriften gehen den Vorschriften der Datenschutzgesetze vor (Art. 2 Abs. 2 BayDSG, § 45 BDSG – am Ende).

Eine Befugnis zur Offenbarung der erbetenen Anschriften kann nur bei Einwilligung der Mutter angenommen werden. Zur Sicherstellung des Nachweises

sollte nur eine schriftliche Form der Einwilligung gewählt werden. Bei der Formulierung der Einwilligung sollten im Interesse der Betroffenen die an anderer Stelle dieses Berichts (siehe unter 3.5) geschilderte Frage der Einwilligung in eine eventuelle bundesweite zentrale Datenspeicherung sowie die Frage der weiteren Nutzung, Übermittlung und Löschung der übermittelten Anschrift durch den Empfänger entsprechend Art. 18 Abs. 5 BayDSG berücksichtigt werden.

3.5 Schul- und Hochschulbereich

3.5.1 Verwendung von Gesundheitskarten bzw. Gesundheitsbogen an Schulen

Vor schulärztlichen Untersuchungen werden Fragebogen in Form von Gesundheitskarten oder Gesundheitsbogen an die Schüler verteilt. Sie sollen dem Schularzt als Unterlage für die Untersuchung dienen. Erfragt werden – nicht an allen Schulen einheitlich – zum Teil höchst sensible medizinische Daten. Die Frage nach der Erforderlichkeit von Daten, die zumindest während der Zeit des Verbleibens des Kindes an der Schule dort aufbewahrt werden, drängt sich beispielsweise auf, soweit nach der Todesursache oder Krankheit von Eltern oder Geschwistern, Frühgeburt, Übertragung, Mehrlingsgeburt, Saugglocke, Zange, Kaiserschnitt – das sind gleichzeitig sehr persönliche Angaben über die Mutter – oder „besonderen Angaben über das Kind oder die Familie“ gefragt wird. Bei den Angaben über dritte Personen muß problematisch erscheinen, daß diese von der Tatsache der jahrelangen Verfügbarkeit dieser Angaben in der Schule nichts erfahren und auf die Richtigkeit der Angaben in der Regel keinen Einfluß nehmen können.

Wichtig erscheint deshalb auch die Sicherung solcher Unterlagen gegen Kenntnisaufnahme Unbefugter. Grundsätzlich dürfen die erhobenen Daten nur dem Schularzt zur Verfügung stehen. Das Bayer. Staatsministerium für Unterricht und Kultus hat u. a. in einer Entschließung vom 27. 6. 1949 (KMBl. S. 118) für Gymnasien vorgesehen, daß Lehrer vom Schularzt so weit unterrichtet werden, wie dies für den Unterricht und die Erziehung des Schülers erforderlich ist. Der Schularzt bleibt aber für die Verwahrung der Unterlagen verantwortlich. Nur er darf die vollständigen Gesundheitsangaben einsehen.

In Nürnberg und bei Stichproben im Münchner Raum hat sich jedoch herausgestellt, daß in Gymnasien die Gesundheitsunterlagen für alle Lehrer offen im allgemeinen Schülerakt geführt und nicht – wie vorgeschrieben – vom Schularzt aufbewahrt wurden. Diese Handhabung wurde beanstandet und gefordert, die Unterlagen – wie vom Kultusministerium vorgeschrieben – in ärztlicher Obhut zu belassen.

Ich bin im übrigen der Ansicht, daß die Erforderlichkeit der Datenerhebung zur rechtmäßigen Aufgabenerfüllung noch im einzelnen geprüft werden muß und daß in den Erhebungsbogen ein eindeutiger Hinweis auf die Verpflichtung zur Angabe von Daten bzw. auf die Freiwilligkeit einzufügen ist (Art. 16 Abs. 2 BayDSG).

3.5.2 Weitergabe von Schülerdaten an Kreditinstitute

Im Berichtsjahr wurden mir drei Fälle bekannt, in denen die Anschriften der Schulanfänger bzw. ihrer Eltern an Kreditinstitute weitergegeben wurden, ohne daß vorher die Einwilligung der Erziehungsberechtigten eingeholt worden wäre.

Solche Datenübermittlungen ohne Einwilligung sind nach § 97 a der Allgemeinen Schulordnung in der Fassung vom 7. 8. 1979 (GVBl. S. 319) unzulässig (wegen Einzelheiten verweise ich auf Nr. 4.1.6.1 meines 2. Tätigkeitsberichts – Seite 22). Nach den Bestimmungen des Bayer. Staatsministeriums für Unterricht und Kultus über das Schulsparen (Bekanntmachung vom 4. 7. 1978 – KMBI. 1978, Seite 431, Textziffern 2.4.2 und 3.4.4) ist die Übermittlung von Anschriften an Kreditinstitute nur mit vorheriger schriftlicher Einwilligung der Erziehungsberechtigten vorgehen.

Soweit das Bayer. Datenschutzgesetz Anwendung findet, d. h. soweit die Anschriften aus einer Datei entnommen wurden, wäre die Übermittlung auch nach Art. 4 i. V. m. § 18 Abs. 1 BayDSG unzulässig. Die Übermittlung ist zur Erfüllung schulischer Aufgaben nicht erforderlich. Auch wenn dem Kreditinstitut ein „berechtigtes“ Interesse nicht abzusprechen ist, so kann doch kein „öffentliches“ Interesse an der Datenübermittlung angenommen werden. Nach der Vollzugsbekanntmachung zu Art. 18 BayDSG (Textziffer 18.2.4) sind Auskünfte über mehrere vom Empfänger nicht namentlich bezeichneter Personen (Gruppenauskünfte) im Regelfall nur zu erteilen, wenn sie im „öffentlichen Interesse“ liegen. Ein öffentliches Interesse fehlt bei der Übermittlung von Daten zu Werbezwecken (so auch Art. 24 Abs. 2 BayDSG für Gruppenauskünfte aus dem Melderegister).

Die Weitergabe der Daten an die Kreditinstitute war deshalb zu beanstanden.

3.5.3 Bezeichnung „Sonderschule“ auf Schülerausweisen

An Sonderschulen wurden bisher Schülerausweise ausgegeben, die den Inhaber als Schüler einer Sonderschule ausweisen. Nachdem die Schülerausweise im wesentlichen zum Nachweis des Schülerstatus für verbilligte Eintrittskarten o. ä. dienen, die Verwendung des Ausweises also an das Tatbestandsmerkmal Sonderschule (im Gegensatz zu normaler Schule) nicht anknüpft, halte ich es für unverhältnismäßig, den Schüler bei jeder Benützung des Ausweises zur Offenbarung seines Sonderschülerstatus zu zwingen. Ich habe deshalb gegenüber dem Bayer. Staatsministerium für Unterricht und Kultus angeregt, einen neutralen Schulbegriff für diese Ausweise zu finden.

3.5.4 Datenerhebung für Kindergarten

In einer Eingabe wurde kritisiert, daß bei der Aufnahme in den Kindergarten Angaben gefordert würden, die nicht erforderlich erschienen. Die von den Eltern auszufüllende Karteikarte enthielt unter anderem die Frage nach Geburtsdatum, Beruf, Geburtsort, Arbeitgeber und Religion des Vaters, denselben Angaben für die Mutter, sowie Angaben über die

Geschwister. Auf meine Anfrage bei der zuständigen Gemeinde nach der Erforderlichkeit der genannten Angaben wurde mir mitgeteilt, daß die Kindergarten-Karteikarten auf die Anfrage hin umgestaltet worden seien. Die angeführten Fragen wurden in dem neuen Formular weggelassen, die bisher verwendeten Karteikarten eingezogen und vernichtet.

3.5.5 Einsichtnahme in Studentenkarteien

Aufgrund einer Eingabe wurde festgestellt, daß Bedienstete von Stellen, an die Daten übermittelt werden sollten, in die Studentenkartei Einsicht genommen und die benötigten Informationen abgeschrieben hatten. Studentenkarteien enthalten zu einem erheblichen Teil Angaben, die auch für die Zwecke der Statistik nach dem Hochschulstatistikgesetz erhoben werden. Einzelne Angaben sind möglicherweise ausschließlich für Zwecke der Hochschulstatistik bestimmt. Die für Zwecke der Hochschulstatistik erhobenen Angaben sind durch § 15 des Hochschulstatistikgesetzes (HStatG) und § 11 des Bundesstatistikgesetzes besonders geschützt. § 15 Abs. 3 HStatG eröffnet die Möglichkeit, die für statistische Zwecke erhobenen Angaben auch „für verwaltungsinterne Zwecke“ zu verwenden. Diese Vorschrift erlaubt jedoch nicht, Dritten die Einsichtnahme in alle Angaben zu gestatten. Die Einsichtgewährung ist daher wegen Verstoßes gegen das Statistikgeheimnis unzulässig.

Soweit neben dem Statistikrecht das BayDSG anzuwenden ist, z. B. hinsichtlich der Angaben in der Kartei die nicht für die Hochschulstatistik erhoben wurden, führt die Überprüfung zum selben Ergebnis. Es steht außer Zweifel, daß die Offenbarung sämtlicher Angaben der Karteikarte zur Erfüllung der Aufgaben der einsichtnehmenden Stelle nicht erforderlich ist. Da die Gewährung der Einsichtnahme aber gemäß Art. 5 Abs. 2 Nr. 2 BayDSG als vollendete Übermittlung sämtlicher Angaben der Karteikarte gilt, ist sie als unzulässig zu betrachten. Anstelle der Einsichtnahme muß deshalb ein anderer Weg gefunden werden, der die Übermittlung auf die zur rechtmäßigen Aufgabenerfüllung erforderlichen Daten beschränkt.

3.5.6 Abiturientenbefragung

Zum Problembereich der Abiturientenbefragung siehe Statistik und Planung (3.6.4).

3.6 Statistik und Planung

3.6.1 Übermittlung und Nutzung von Statistikdaten für sonstige Verwaltungszwecke

Nach Art. 23 Abs. 2 BayDSG dürfen personenbezogene Daten, die für amtliche Statistiken erhoben wurden, an andere Stellen nur soweit übermittelt werden,

- als es die die statistische Erhebung anordnende Rechtsvorschrift zuläßt und soweit dies
- in Erhebungsdrucksachen bekanntgegeben wurde.

Das Bundesstatistikgesetz schreibt in § 11 Abs. 3 dasselbe für den Umgang mit Daten vor, die für eine Bundesstatistik erhoben wurden.

Die Verwendung der im Zuge der amtlichen Viehzählung erhobenen Angaben über persönliche oder sachliche Verhältnisse des Tierhalters zur Abrechnung der Tierseuchenbeiträge gemäß Art. 3 Abs. 2 des Gesetzes über den Vollzug des Tierseuchenrechts vom 8. 4. 1974 (GVBl. S. 152, geändert GVBl. 1978 S. 335) setzt deshalb voraus, daß diese Verwendung der Angaben im Viehzählungserhebungsbogen „bekanntgegeben“ wird. Das Bayer. Statistische Landesamt weist deshalb neuerdings auf der Rückseite des Erhebungsbogens unter der Überschrift „Geheimhaltung“ auf diese Verwendung hin. Es hat außerdem auf meine Anregung hin mitgeteilt, daß auf der Vorderseite des Erhebungsbogens ein deutlicher Hinweis auf die Erläuterungen auf der Rückseite angebracht werden wird. Ich halte dies für erforderlich, da der Tierhalter selbst in aller Regel keine Kenntnis vom Text auf der Rückseite nimmt.

3.6.2 Nutzung von Verwaltungsdaten für Planungszwecke

Im Tätigkeitsbericht des vergangenen Jahres wurde unter der Textziffer 4.1.3.1 die Problematik von Datensammlungen mit personenbezogenen Daten für Planungsbehörden angesprochen. Im Berichtszeitraum war die Tendenz festzustellen, daß im kommunalen Bereich zunehmend Individualdaten für Planungszwecke gespeichert werden. Als Datenquellen werden neben freiwilligen Erhebungen Angaben aus dem automatisierten Einwohner- und Kfz-Zulassungswesen herangezogen. Die Zulässigkeit der Datenübermittlung beurteilt sich gem. Art. 17 Abs. 3 Satz 2 nach Art. 17 Abs. 1 BayDSG.

Umstritten ist nach wie vor die Speicherung des vollen Namens (Familiename und Vorname) für Zwecke der kommunalen Statistik. Die Speicherung dieses Merkmals wird von den Planern häufig damit begründet, daß es zusammen mit dem Geburtsdatum und der Adresse zur Zusammenführung von Datenbeständen diene. Ich bin der Meinung, daß eine Speicherung des Namens nach der Zusammenführung von Datenbeständen grundsätzlich nicht mehr notwendig ist. Für weitere Verknüpfungen, die bei der Datenübermittlung noch nicht vorhersehbar sind, halte ich es für datenschutzgerechter, wenn das über ein planungsamts-internes Identifizierungsmerkmal geschieht und somit die Bestimmbarkeit der einzelnen Person bei der planenden Stelle ohne Zuhilfenahme der Datenbestände des Vollzugs unmöglich bzw. nur mit großem Aufwand ermöglicht wird. Die Umsetzung des Namens in das planungsamts-interne Identifizierungsmerkmal könnte mit einer besonders geschützten Datei erfolgen.

Diese Problematik soll auch in der Datenschutzstudie zum sogenannten „Penta-Projekt“ behandelt werden. Das „Penta-Projekt“ ist ein Forschungsvorhaben zur Entwicklung von Methoden und Verfahren für Planungs- und Entscheidungshilfen auf der Basis des automatisierten Einwohnerwesens. Mit der Projektentwicklung ist das Institut für ADV-gestützte Entwicklungsplanung DATUM e.V. beauftragt. Zu den Pilotanwendern zählen aus dem öffentlichen Bereich des Freistaates Bayern die Anstalt für kommunale

Datenverarbeitung, das Bayer. Staatsministerium für Landesentwicklung und Umweltfragen sowie die Stadt Nürnberg. In einer inzwischen von DATUM vorgelegten Datenschutzstudie wurden konkrete Vorschläge über den Daten- und Methodenkranz gemacht, außerdem wurden erste Hinweise über die rechtlichen Voraussetzungen für die Speicherung solcher Individualdaten beim Statistischen Amt einer Kommune gegeben. Als Identifizierungs- und Verknüpfungsmerkmal wird zwar der Name vorgeschlagen, durch besondere technische Sicherungsmaßnahmen soll aber für den Planer der Zugriff auf den Namen im Einzelfall ausgeschlossen werden. Es ist vorgesehen, diese Studie im Kreis der Länderbeauftragten zu diskutieren.

Werden von einer öffentlichen Stelle personenbezogene Daten an eine zentrale statistische Stelle übermittelt, sollte die Prüfung, inwieweit diese personenbezogenen Daten zur Erfüllung der Aufgaben der statistischen Stelle erforderlich sind, grundsätzlich nicht nur durch diese Stelle, sondern auch durch eine unabhängige Stelle – geeignet wäre z. B. der behördliche Datenschutzbeauftragte – geprüft werden.

Prüft die übermittelnde Stelle die Erforderlichkeit, so ist ihr generell der Zweck mitzuteilen, für welche Aufgaben die empfangende Stelle die übermittelten Daten benötigt. Ebenso ist es für die übermittelnde Stelle wichtig zu erfahren, wie lange die übermittelten Daten bei der empfangenden Stelle als Individualdaten gespeichert werden.

In allen Fällen, bei denen neue Datenarten in das statistische System eingespeist werden sollen, ist eine Freigabe nach Art. 26 Abs. 2 BayDSG erforderlich.

3.6.3 Erhebung von Namen und Anschriften der Betroffenen für die Sozialhilfestatistik

Die Sozialhilfestatistik ist durch das Gesetz über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsofopferfürsorge und der Jugendhilfe vom 15. 1. 1963 (BGBl. I S. 49), geändert durch Art. 19 des 1. Gesetzes zur Änderung statistischer Rechtsvorschriften vom 14. 3. 1980 (BGBl. I S. 294), geregelt. Dieses Gesetz sieht die Erhebung der Namen und Anschriften von Sozialhilfeempfängern für die Sozialhilfestatistik nicht vor. Die Erhebung und Speicherung von Namen und Anschrift der Hilfeempfänger, wie sie bisher von den Statistischen Ämtern in der Bundesrepublik durchgeführt wurde, entbehrt daher der Rechtsgrundlage.

Auf meine Bitte hat deshalb auch das Bayer. Statistische Landesamt, wie die Statistischen Ämter anderer Bundesländer, veranlaßt, daß Namen und Anschrift der Sozialhilfeempfänger für die Statistik nicht mehr erhoben werden. Für die laufende Erhebung im Jahr 1980 wurden die Erhebungsstellen gebeten, Namen und Anschrift nicht mehr mitzuteilen, obwohl sie auf dem Erhebungsbogen noch vorgesehen sind.

3.6.4 Schülerbefragung im Absolventenjahrgang der Sekundarstufe II (Abiturientenbefragung)

In der Eingabe mehrerer Schüler ist Beschwerde darüber geführt worden, daß für die Befragung über

die Studien- und Berufswünsche von Abiturienten die Bekanntgabe des Namens des Schülers gegenüber dem Statistischen Landesamt gefordert wird.

Das Bundeshochschulstatistikgesetz vom 31. 8. 1971 ermächtigt zur Erhebung von „Angaben zur Person“. Angaben zur Person können grundsätzlich Name und Adresse sein, aber auch Angaben, die eine Person zwar beschreiben, sie aber ohne ein bestimmtes Maß an verfügbaren Zusatzwissen nicht bestimmbar werden lassen, wie z. B. Alter, Geschlecht, Einzelkind o. ä. Welche Angabe für die konkrete Statistik erhoben werden muß ist deshalb anhand des Zweckes der Statistik zu beurteilen.

Zweck der Erhebung über Studien- und Berufswünsche ist es, jährlich alle Schüler der Sekundarstufe II unter Benutzung des Datenmaterials über die Studien- und Berufswünsche der übrigen Schüler eines Absolventenjahrgangs zu informieren und damit eine Orientierungshilfe für die Studienwahl zu geben. Außerdem sollen die gewonnenen Zahlen für die mittelfristige Kapazitätsplanung im Hochschulwesen dienen. Um den ersteren Zweck zu erfüllen, müssen die Ergebnisse der im Frühjahr durchzuführenden Erhebung vorliegen, bevor die Abiturienten die Schulen verlassen. Da es sich um eine Erhebung von Studien- und Berufs-„Wünschen“ handelt, können keine exakten Tatsachen oder Zahlen erfragt werden. Die Einbeziehung der erhobenen Daten in eine Verlaufstatistik ist nicht vorgesehen. Die Ermächtigung im Hochschulgesetz würde hierzu, mangels ausreichender Bestimmtheit, wohl auch nicht ausreichen.

Meiner Ansicht nach ist das Hochschulstatistikgesetz, das die Erhebung des Namens nicht vorschreibt, nach dem Grundsatz der Verhältnismäßigkeit so auszulegen, daß jedenfalls bei dieser Erhebung der Name dem Statistischen Landesamt nicht bekanntzugeben ist. Die Vollzähligkeitskontrolle kann ohne nennenswerten belastenden Aufwand mit Namenslisten, die die Schulen führen, sichergestellt werden. Es wird für unwahrscheinlich gehalten, daß angesichts der kurzen Zeit zwischen Erhebung und Bekanntgabe der Ergebnisse Rückfragen des Statistischen Landesamts erforderlich werden. Für diesen Zweck könnten erforderlichenfalls numerische Ordnungsmerkmale von der Schule an das Statistische Landesamt mitgeteilt werden. Bei Auswertungen von so unsicheren Angaben wie „Wünschen“ wird im übrigen von der Statistik häufig bewußt eine Unschärfe eingebaut, die die Auswirkung von besonders aus dem Rahmen fallenden und unwahrscheinlichen Angaben auf das statistische Ergebnis mildert.

Die Statistischen Ämter der Bundesrepublik waren zur Frage der Bekanntgabe des Namens nicht einheitlicher Meinung. Einige Ämter halten die Bekanntgabe für die genannte Statistik für entbehrlich. Sie weisen in diesem Zusammenhang darauf hin, daß sich immer mehr Schüler weigern, ihren Namen auf den Erhebungsbogen anzugeben. Die Statistischen Ämter der Bundesrepublik haben sich deshalb in einer Besprechung darauf geeinigt, daß die Frage nach dem Namen des Schülers zwar auf dem einheitlichen Erhebungsbogen der Abiturientenbefragung enthalten bleiben solle, den einzelnen Statistischen

Landesämtern jedoch freigestellt werde, wenn die Vollzähligkeit der Bogen auf andere Weise gewährleistet werden könne, in Erläuterungen und Begleitschreiben zur Erhebung darauf hinzuweisen, daß auf die Angabe des Namens des Befragten verzichtet wird. Der Saarländische Landesbeauftragte für den Datenschutz hat deshalb die Übermittlung des Namens an das Statistische Landesamt bereits beanstandet. Soweit bisher bekannt geworden, wird im Saarland, in Baden-Württemberg und Rheinland-Pfalz auf die Mitteilung des Namens an das Statistische Landesamt verzichtet. Ich habe dem Bayerischen Statistischen Landesamt und dem Bayerischen Staatsministerium für Unterricht und Kultus empfohlen auf die Bekanntgabe des Namens ebenfalls zu verzichten, um den bestehenden Bedenken einer gegen den Verhältnismäßigkeitsgrundsatz verstoßenden Auslegung des Statistikgesetzes Rechnung zu tragen.

3.7 Personalwesen

3.7.1 Zulässigkeit der Registrierung dienstlicher Telefongespräche

Das Bayer. Staatsministerium des Innern hat gegenüber einer Stadt — meiner Ansicht nach zu Recht — die Ansicht vertreten, daß die Registrierung dienstlicher Telefongespräche auch ohne Einwilligung des Bediensteten zulässig ist. Die Rechtfertigung zur Registrierung dienstlicher Telefongespräche wird aus dem Dienstverhältnis abgeleitet. Es muß dem Dienstherrn möglich sein, den Umfang dienstlich geführter Telefongespräche zu Abrechnungszwecken zu erfassen.

Zu prüfen wird noch sein, ob bei bestimmten Behörden eine differenziertere Betrachtungsweise hinsichtlich der Registrierung der angerufenen Telefonnummer erforderlich ist. Was bei einer Gemeindeverwaltung in der Regel unproblematisch ist, könnte beispielsweise bei Personen, die der ärztlichen Schweigepflicht unterliegen, anders zu beurteilen sein. Als Argument gegen die Registrierung der angerufenen Telefonnummer wird u. a. geltend gemacht, daß durch einen Kontrollanruf bei dieser Nummer ein Bezug der angerufenen Person zu einer besonders zur Verschwiegenheit verpflichteten Dienststelle bekannt würde.

Ungeklärt ist gegenwärtig noch die Frage der Registrierung privater Telefongespräche nach den angerufenen Nummern. Bedenken werden hier einmal dadurch ausgelöst, daß der Dienstherr durch die Registrierung die Beziehungen des Bediensteten zu bestimmten Personen oder Stellen dokumentieren würde und auch überprüfen könnte, zum anderen dadurch, daß auch die schutzwürdigen Belange des durch die Telefonnummer möglicherweise identifizierten Dritten zu berücksichtigen sind. Während eine Einwilligung des Bediensteten grundsätzlich eingeholt werden könnte, scheidet diese Möglichkeit beim angerufenen Dritten aus.

3.7.2 Weitergabe der Anschriften von Bewerbern für die Beamtenlaufbahn an Versicherungen

Im Berichtsjahr sind erneut Beschwerden darüber eingegangen, daß Versicherungsvertretern die An-

schriften von Beamtenanwärtern zur Verfügung stehen. Ich verweise hierzu auch auf meine Ausführungen im 2. Tätigkeitsbericht (Seite 23 Nr. 4.1.7). Eine abschließende Klärung war bisher leider immer noch nicht möglich.

3.7.3 Personalnachrichten der staatlichen Bibliotheken

Die mehrmals jährlich erscheinenden Personalnachrichten der Generaldirektion der Bayer. Staatlichen Bibliotheken enthalten personenbezogene Daten aus Dateien (Diensteintritt, Versetzungen, Beförderungen u. ä.). Die Nachrichten werden an die staatlichen Bibliotheken und an das Personal der Bibliotheken verteilt. Die Übermittlung an andere bayerische staatliche Bibliotheken wurde nach Art. 17 Abs. 1 BayDSG grundsätzlich für zulässig erachtet. Es wurde davon ausgegangen, daß die Nachricht über die personellen Veränderungen für die Erfüllung der Aufgaben der Personalverwaltung in den jeweiligen Bibliotheken zumindest zur Wahrung des Gleichbehandlungsgrundsatzes erforderlich ist. Die Übermittlung an einzelne Bibliotheks-Bedienstete wird aufgrund von Art. 18 Abs. 1, 2. Alternative BayDSG für zulässig gehalten. Bei diesem Empfängerkreis ist ein berechtigtes Interesse an der Transparenz der Personalpolitik festzustellen. Schutzwürdige Belange der Betroffenen werden durch eine solche Übermittlung m. E. nicht beeinträchtigt, da die Empfänger der Personalnachrichten zum Kreis des Personals der Bayerischen Staatlichen Bibliotheken gehören, über das in den Personalnachrichten berichtet wird.

3.7.4 Aufbewahrung von Gleizeit-Erfassungskarten

Verschiedentlich wurde ich auf Fragen der Datensicherung bei der Aufbewahrung von Gleizeiterfassungskarten angesprochen. Generell ist festzustellen, daß die Sammlung dieser Karten nach Art. 5 Abs. 3 Nr. 3 BayDSG als Datei im Sinne der Datenschutzgesetze anzusehen ist, so daß sich die Datensicherungsmaßnahmen nach Art. 15 Abs. 1 BayDSG richten. In der Vollzugsbekanntmachung über Maßnahmen zur Datensicherung (MABl. Nr. 3/1979, Seite 31) sind auch Maßnahmen für nicht automatisierte Verfahren vorgesehen: Nr. 3.3.1 legt fest, daß Dateien so aufzubewahren sind, daß Unbefugte deren Inhalt weder einsehen, verändern oder löschen, noch deren Datenträger entwenden oder zerstören können. Ferner ist zu gewährleisten, daß personenbezogene Daten nicht unbefugt zur Kenntnis genommen werden können (Nr. 3.2.1).

Die Karteikästen, in denen die Gleizeit-Erfassungskarten des Behördenpersonals aufbewahrt werden, sind oft in der Nähe des Hauseingangs so angebracht, daß sie unbefugten Dritten zugänglich sind (z. B. Publikumsverkehr, Reinigungspersonal, Handwerker). Ein Mißbrauch der Zeit-Daten ist deshalb nicht ausgeschlossen. Grundsätzlich anzustreben wäre demgegenüber eine räumliche Abschottung gegenüber behördenfremden Personen.

Da dies in einem überprüften Fall nicht durchführbar war, wurde vorgeschlagen, auf den Gleizeit-Erfassungskarten anstatt des Namens des Bediensteten nur eine neutrale Nummer einzutragen und es dem

Bediensteten freizustellen seinen Namen einzutragen und die Karten bei sich zu tragen. Ein Deponieren der Karten in den Karteikästen erfolgt freiwillig. Im nächsten Tätigkeitsbericht wird über die Erfahrung mit dem gewählten Verfahren berichtet werden.

3.7.5 Veröffentlichung von Angaben über Behördenpersonal in Adreßbüchern

In Adreßbüchern war es teilweise üblich, Angaben über das Personal der örtlichen Behörden in einer Art Behördenwegweiser zu veröffentlichen. Ich habe gegenüber Gemeinden, die von Adreßbuchverlagen um entsprechende Personaldaten gebeten worden waren, die Ansicht vertreten, daß hierfür die Einwilligung zumindest derjenigen Bediensteten einzuholen wäre, die nicht als Leiter der jeweiligen Behörden, Ämter oder verselbständigten Dienststellen, oder deren Stellvertreter, oder in sonstiger Weise öffentlich bekannte, in ihrer Funktion besonders herausgehobene Mitarbeiter anzusehen sind. Die Einwilligung sollte zumindest vorsorglich eingeholt werden, da nicht auszuschließen ist, daß durch eine solche Übermittlung und Veröffentlichung schutzwürdige Belange der in der Öffentlichkeit nicht in Erscheinung tretenden Bediensteten beeinträchtigt werden (Art. 18 Abs. 1, 2. Alternative BayDSG). Außerdem bestehen auch Zweifel, ob der Übermittlung und Veröffentlichung von Angaben über diese Personen ein ausreichendes öffentliches Interesse zur Seite steht (Vollzugsbekanntmachung zu Art. 18 BayDSG, Textziffer 18.2.4).

In einem von mir kritisierten Fall war die Veröffentlichung beispielsweise von Angaben über 12 Mitarbeiter des Stadtkämmerers, über den Amtsoffizianten, die Telefonzentrale, die Angestellte der Volksschule sowie von Privatanschriften und -telefonnummern Bediensteter vorgesehen.

3.8 Berührungspunkte mit öffentlich-rechtlichen Religionsgesellschaften

Die Anwendbarkeit des Bundesdatenschutzgesetzes und des Bayerischen Datenschutzgesetzes auf öffentlich-rechtliche Religionsgesellschaften, deren rechtlich selbständige Teile sowie auf sonstige ihnen zugeordnete Einrichtungen ist noch nicht abschließend geklärt. Die Anwendbarkeit der Datenschutzgesetze hängt u. a. von der Organisationsform der einzelnen kirchlichen Einrichtung, dem jeweiligen Tätigkeitsfeld und den im Einzelfall den öffentlich-rechtlichen Religionsgesellschaften verliehenen Befugnisse ab. Die Gesetzgeber der Datenschutzgesetze sind grundsätzlich davon ausgegangen, daß die öffentlich-rechtlichen Religionsgesellschaften den Datenschutz im Rahmen ihrer durch Artikel 140 Grundgesetz in Verbindung mit Art. 137 Weimarer Verfassung verfassungsrechtlich gesicherten Autonomie selbst regeln. Tatsächlich haben die katholische und die evangelische Kirche entsprechende datenschutzrechtliche Regelungen getroffen. Sind den öffentlich-rechtlichen Religionsgesellschaften jedoch staatliche Befugnisse verliehen, wie z. B. im Schul- oder Friedhofswesen, so sind sie insoweit grundsätzlich Behörden mit der Folge, daß die jeweiligen Datenschutzgesetze unmittel-

bar auf sie anwendbar sind. Soweit Einrichtungen der öffentlich-rechtlichen Religionsgesellschaften selbstständig in bürgerlich-rechtlicher Form organisiert sind, kann im Einzelfall die Anwendbarkeit des Bundesdatenschutzgesetzes in Betracht kommen.

Die Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften ist nach Art. 25 BayDSG zulässig, soweit die öffentlich-rechtlichen Religionsgesellschaften die Daten zur Erfüllung ihrer öffentlichen Aufgaben benötigen und einen ausreichenden Datenschutz sichergestellt haben. Die letztere Feststellung zu treffen dürfte, dies haben auch an mich gerichtete Schreiben ergeben, insbesondere Gemeinden überfordern. Ich würde es daher begrüßen, wenn die nach Nr. 25.4 Vollzugsbekanntmachung zum Bayer. Datenschutzgesetz auf Antrag durch die Staatsministerien des Innern und für Unterricht und Kultus vorzunehmende Feststellung, daß bestimmte öffentlich-rechtliche Religionsgesellschaften die Datenschutzerfordernungen erfüllen, bald vorgenommen werden könnte. Anhaltspunkte dafür, daß öffentlich-rechtliche Religionsgesellschaften keinen ausreichenden Datenschutz sicherstellen, habe ich nicht.

3.9 Neue Medien

Die Einführung der „Neuen Medien“ kann zu erheblichen datenschutzrechtlichen Gefahren führen. Ich will nur auf die mögliche Erstellung umfassender Persönlichkeitsprofile und die Ansammlung umfangreicher Bestände personenbezogener Daten hinweisen. Den denkbaren Gefahren gilt es rechtzeitig zu begegnen. Deshalb haben die Datenschutzbeauftragten der Länder und des Bundes eine Arbeitsgruppe gebildet, die einen ersten Forderungskatalog aus datenschutzrechtlicher Sicht vorlegt.

3.9.1 Anwendungen

Unter dem Begriff „Neue Medien“ werden derzeit technische Entwicklungen diskutiert, die auch Gegenstand der Untersuchung im Telekommunikationsbericht der Kommission für den Ausbau des technischen Kommunikationssystems gewesen sind. Hierzu zählen die durch Breitbandkabelnetze gegebene Möglichkeit eines vergrößerten und programmlich anders gestalteten Rundfunkangebots und der neuen Darstellungsform von Texten auf dem Bildschirm wie Videotext, Bildschirmtext und Kabeltext, das Kabelfernsehen und der Einsatz von Fernseh-Rundfunksatelliten. Die Ministerpräsidenten der Länder haben am 11. Mai 1978 die gemeinsame Durchführung und Auswertung von vier Pilotprojekten beschlossen. Als Standorte waren neben München die Städte Berlin, Ludwigshafen-Mannheim und Dortmund vorgesehen. Zwischenzeitlich haben in Berlin und Düsseldorf erste Feldversuche mit Bildschirm- und Video-Text begonnen. Die Bayerische Staatsregierung hat am 14. Juni 1980 die Durchführung eines Versuchs zum Kabelfernseh-pilotprojekt München beschlossen. Die Mitglieder der Projektkommission sind bereits berufen.

Zu den einzelnen Verfahrensarten ist folgendes zu bemerken:

Im Videotext-Verfahren werden codierte Informationen in das Fernsignal der Sender einbezogen

(und über den ohnehin schon vorhandenen Übertragungsweg vom Sender zum Empfänger übertragen). Dabei wird die sogenannte „Austastlücke“ genutzt. Die so übermittelten Informationen können durch ein Zusatzgerät auf dem Bildschirm in Form von Schrift oder Graphikzeichen entweder zusätzlich zum Fernsehbild oder statt des Fernsehbildes sichtbar gemacht werden. Wegen der beschränkten Aufnahmekapazität der „Austastlücke“ ist die Menge der insoweit zu übersenden Informationen begrenzt.

Bildschirmtext wird über ein sogenanntes schmalbandiges Netz, z. B. über das Fernsprechnet der Bundespost, übermittelt. Diese Textinformationen können durch zusätzliche technische Einrichtungen am Bildschirm sichtbar gemacht werden. Im Gegensatz zum beschränkten Angebot bei Videotext-Verfahren kann der Teilnehmer beim Bildschirmtext aus der technisch fast unbeschränkten Zahl von Informations-Angeboten wählen, was er sich auf den Bildschirm holen will. Dies kann auch eine in etwaigen angeschlossenen Datenspeichern enthaltene Information sein.

Beim Kabeltext werden Informationen über ein breitbandiges Netz übertragen. Vor Einführung des Kabeltextes müssen entsprechend leistungsfähige breitbandige Kabelnetze verlegt werden. Derartige Netze sollen gerade bei den vorgenannten vier Kabelfernseh-pilotprojekten der Länder eingerichtet werden. Die Nutzungsmöglichkeiten des Kabeltextes sind vielfältigster Art und reichen von der individuellen selektiven Zugriffsmöglichkeit auf Informationen, ähnlich wie beim Bildschirmtext, bis hin zu ständigen Textprogrammen, die gleichzeitig an alle Teilnehmer gerichtet und für alle jederzeit zugänglich sind.

Bildschirmtext und Kabeltext eröffnen die Einrichtung eines sog. Rückkanals. Der Rückkanal gestattet neben dem Abruf einzelner Informationen von einer Zentrale durch den Teilnehmer auch einen, wenn auch begrenzten Dialog zwischen Teilnehmer und Zentrale. Damit sind zumindest die technischen Voraussetzungen gegeben, daß sich der einzelne am Programm beteiligt, indem er etwa eine laufende Sendung beurteilt oder aktiv auf angebotene Informationen zugreift und beispielsweise Bestellungen auf Versandangebote hin tätigt.

3.9.2 Pilotprojekt in Bayern

Voraussetzung für den Beginn des Pilotprojektes in München ist die Verlegung eines breitbandigen Netzes. Nach dem derzeitigen Stand der Überlegungen dürfte mit dessen Inbetriebnahme im Jahre 1983 zu rechnen sein. Das Versorgungsgebiet in München, das durch die Verkabelung erschlossen werden soll, wird etwa 46 000 Haushalte umfassen. Wird hierbei von einer Anschlußquote von etwa 20 Prozent ausgegangen, so dürften etwa 10 000 Privathaushalte in das Pilotprojekt einbezogen werden. Die Laufzeit des Pilotprojektes soll etwa 3—5 Jahre betragen. Die rundfunkrechtliche Verantwortung für das Pilotprojekt beabsichtigt die Bayerische Staatsregierung dem Bayerischen Rundfunk unter gleichberechtigter Mitwirkung des Zweiten Deutschen Fernsehens zu übertragen. In einer Rahmenvereinbarung mit dem Bayerischen

Rundfunk und dem Zweiten Deutschen Fernsehen sollen die Grundsätze über die Planung, Organisation und Durchführung des Modellversuches festgelegt werden. Weil die Rundfunkanstalten von ihrer Aufgabenstellung her nur für die Veranstaltung von Rundfunk, d. h. Hörfunk und Fernsehen, zuständig sind, soll die Verantwortung für andere im Pilotprojekt angebotene Dienste nicht den Rundfunkanstalten übertragen werden. Deshalb muß für die „gemeinsame Betriebszentrale“, in die alle Informations-Angebote eingebracht und von der aus alle Dienste angeboten werden können, eine besondere Organisationsform gefunden werden.

3.9.3 Datenschutzrechtliche Probleme

Die Einführung der Neuen Medien kann datenschutzrechtliche Gefahren mit sich bringen, deren Umfang derzeit noch nicht exakt übersehbar ist. Die Neuen Medien werden zu einer verstärkten Kommunikation zwischen Anbietern und Benutzern führen. Diese verstärkte Kommunikation dürfte auch dazu führen, daß insbesondere über den Benutzer eine Reihe von personenbezogenen Daten anfallen. So lassen sich grundsätzlich bei einer gemeinsamen Betriebszentrale Art und Umfang der vom einzelnen Benutzer angerufenen Programmangebote feststellen: Rückschlüsse auf den einzelnen Benutzer und dessen Lebensäußerungen sind grundsätzlich auch über die Benutzung des Rückkanals möglich. Schließlich könnte in der Betriebszentrale registriert werden, wie sich der einzelne Benutzer beim Abfragen der ihm zur Verfügung stehenden Angebote verhalten hat und welche Geschicklichkeit er hierbei bewiesen hat. Dabei ist datenschutzrechtlich nicht allein problematisch, daß über die Benutzung der Neuen Medien eine Vielzahl von einzelnen Informationen über den einzelnen Benutzer anfällt, vielmehr ist es besonders gefährlich, daß sich über diese Daten Interessen- und Persönlichkeitsprofile erstellen ließen. An den hierbei gewonnenen Informationen könnte im Bereich der Privatwirtschaft wie auch im Bereich der öffentlichen Verwaltung oder der Polizei starkes Interesse bestehen.

Um möglichst bereits bei den Pilotprojekten feststellen zu können, ob die vermuteten datenschutzrechtlichen Gefahren tatsächlich auftreten oder nicht erkannte neue Risiken erkennbar werden, muß bereits im Rahmen der Pilotprojekte eine datenschutzrechtliche Begleituntersuchung stattfinden. Darüber hinaus muß auch bereits bei den Pilotprojekten der Datenschutz beachtet werden. Wie weitgehend hier die Datenschutzerfordernisse sein müssen, kann erst entschieden werden, wenn das Konzept für das Pilotprojekt feststeht. Hierbei ist zu bedenken, daß durch zu hohe Datenschutzerfordernisse für die Projektierungsphase mögliche Gefahren, die bei einem Echtbetrieb auftreten können, nicht entdeckt werden. Andererseits besteht das Risiko, daß während der Projektierungsphasen eingespielte Verfahrensweisen, in denen der Datenschutz nicht ausreichend berücksichtigt wird, in einem späteren Echtzeitbetrieb als bereits bewährt übernommen werden, ohne daß dann für erforderlich gehaltene Datenschutzmaßnahmen noch in die Verfahren einbezogen werden können.

Ich bin gerne bereit, an den hierzu notwendigen Überlegungen mitzuwirken.

Vorbehaltlich näherer Erkenntnisse über die technische Verwirklichung der Neuen Medien im einzelnen und der hierbei erst noch deutlich werdenden Datenschutzgefahren haben die Datenschutzbeauftragten des Bundes und der Länder die nachfolgenden Grundsätze für den Datenschutz bei den Neuen Medien unter besonderer Berücksichtigung von Bildschirmtext und Kabelfernsehen verabschiedet.

3.9.4 Grundsätze für den Datenschutz

Vorbemerkung

Die nachstehenden Grundsätze für den Datenschutz bei den Neuen Medien sollen sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrunde liegenden Vorschriften den Datenschutz von vornherein berücksichtigen und dieser dem Einsatz neuer Technologien nicht nachfolgt.

Die Grundsätze können dem Stand der Vorhaben und der technischen Entwicklung entsprechend nicht abschließend sein.

1. Informationssammlung über Teilnehmer

1.1 Bei der Einführung Neuer Medien ist der Datenschutz sicherzustellen. Dies gilt auch für die Versuchsphase. Bereits hierfür sollten gesetzliche Regelungen getroffen werden.

1.2 Personenbezogene Benutzerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit ihre Verarbeitung für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen der Neuen Medien nicht durchgeführt werden kann.

1.3 Der Schutz der in den Neuen Medien anfallenden personenbezogenen Teilnehmerdaten kann nicht auf deren Verarbeitung in Dateien beschränkt werden.

1.4 Sofern bei bestimmten Diensten eine unmittelbare Teilnehmer-Anbieter-Kommunikation vorgesehen ist, dürfen Daten nur in dem Umfang festgehalten und übermittelt werden, wie dies zur Durchführung des jeweiligen Dienstes erforderlich und aufgrund der einschlägigen gesetzlichen Regelung zulässig ist.

1.5 Gebühren und Entgelte sind in anonymer Form zu berechnen und abzurechnen, soweit eine individualisierbare Registrierung von einzelnen Kommunikationsvorgängen zur Abwicklung von Vertragsverhältnissen nicht erforderlich ist. Sollte eine zusätzliche Kontrolle erforderlich werden, so könnte beim Benutzer eine Zählereinrichtung installiert werden.

2. Bedeutung des Versuchsstadiums (Pilotprojekte)

2.1 Bereits in der Versuchsphase ist ein möglichst wirksamer Datenschutz sicherzustellen, da diese Phase die spätere Nutzung der Neuen Medien prägt.

2.2 In der Versuchsphase ist zu prüfen, ob weitere Datenschutzregelungen auf dem Gebiet der Neuen Medien nötig sind oder ob vorhandene Vorschriften modifiziert werden müssen.

2.3 Im Rahmen wissenschaftlicher Begleituntersuchungen ist dafür zu sorgen, daß auch die Datenschutzfragen besonders geprüft werden.

2.4 Im Rahmen einer wissenschaftlichen Begleituntersuchung ist der Zugriff auf gespeicherte Datenbestände nur gestattet, sofern diese Daten anonymisiert worden sind. Darüber hinausgehende Daten dürfen nur von den Teilnehmern direkt erfragt werden.

Die Datenverarbeitung sollte in allen Phasen nur mit Einwilligung des Teilnehmers erfolgen (vgl. dazu Ziff. 3).

3. Die Bedeutung der „Einwilligung“ bei der Speicherung von Teilnehmerdaten

3.1 Die Speicherung von Teilnehmerdaten in einer Form, die die Erstellung individueller Persönlichkeitsprofile gestattet, ist zu verbieten. Darüber hinaus kann in einzelnen Diensten die Speicherung besonders sensibler Daten aus dem „unantastbaren Bereich privater Lebensgestaltung“ (vgl. BVerfGE 27, 7; s. a. § 27 Abs. 3 Satz 3 BDSG) grundsätzlich verboten werden. Eine Einwilligung des Teilnehmers hebt das Verbot nicht auf.

3.2 Im übrigen ist eine Speicherung von Teilnehmerdaten erlaubt,

- a) wenn eine gesetzliche Regelung dies zuläßt;
- b) wenn der Teilnehmer seine Einwilligung gibt.

Diese Einwilligung ist nur wirksam, wenn der Teilnehmer zuvor sorgfältig über ihre Konsequenzen aufgeklärt worden ist (informed consent). Dies gilt auch für den Abschluß von Verträgen.

4. Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können

4.1 Nutzungsmöglichkeiten des Rückkanals und aller sonstigen technischen Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können, sollen nach Möglichkeit gesetzlich geregelt werden. Soweit Teilnehmerdaten gespeichert werden können, dürfen sie nur zu dem Zweck verwendet werden, zu dem sie offenbart wurden.

4.2 Persönlichkeitsprofile der Teilnehmer dürfen anhand der in der Betriebszentrale anlaufenden Kommunikationsdaten nicht erstellt werden. Dies gilt für jede Betriebszentrale, unabhängig von der angewendeten Technologie.

4.3 Abstimmungen und Wahlen über den Rückkanal dürfen nicht durchgeführt werden.

5. Medienprivileg

5.1 Das Verhältnis des Medienprivilegs zu den Neuen Medien bedarf insgesamt einer eingehenden Untersuchung.

5.2 Dabei muß insbesondere geprüft werden,

- ob die einzelnen Neuen Medien als Presse bzw. Rundfunk anzusehen sind oder ob es sich um Medien sui generis handelt,
- in welchen Fällen nach geltendem Recht personenbezogene Daten ausschließlich zu publizistischen Zwecken verarbeitet werden,
- ob der Geltungsbereich des Medienprivilegs im Hinblick auf die für die Benutzer bestehenden Gefahren sachgerecht geregelt ist,
- falls dies bejaht wird: ob der Geltungsbereich zur Klarstellung gesetzlich geregelt werden soll,
- falls dies verneint wird: inwieweit der Geltungsbereich neu geregelt werden sollte.

Schließlich bedarf besonderer Erörterung die Gefahr, daß in Medienarchiven gespeicherte, personenbezogene Daten in die Speicherzentralen eingegeben werden und unter Berufung auf das Medienprivileg (§ 1 Abs. 3 BDSG und entsprechende Regelungen in den Ländergesetzen) frei zugänglich gemacht werden. Unter diesem Gesichtspunkt verdienen auch die im Urteil des Bundesverfassungsgerichts vom 5. Juni 1973 – 1 BvR 536/72 – (BVerfGE 35, S. 202 ff. [219 ff.] „Lebach“) aufgestellten Grundsätze zum Schutze der Persönlichkeit vor dem Zugriff der Öffentlichkeit besondere Berücksichtigung.

6. Fernmeldegeheimnis und Neue Medien

6.1 Im gesamten Netzbereich werden die zentralen Einrichtungen der Neuen Medien ebenso wie die Übertragungswege vom Fernmeldegeheimnis im Sinne von Art. 10 GG umfaßt, sofern es sich dabei um juristische Personen des öffentlichen Rechts handelt.

6.2 Folgt man der Auffassung, daß die zentralen Einrichtungen der Neuen Medien keine Fernmeldeanlagen sind, ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis für den Nutzungsbereich – unter Umständen in Verfassungsrang – zu schaffen.

6.3 Die Einblicknahme in und die Übermittlung von personenbezogenen Daten aus Speichereinrichtungen einer Bildschirmtext- bzw. Kabelfernsehzentrale sind nur aufgrund gesetzlicher Regelungen unter engen, genau bestimmten Voraussetzungen zulässig. Unter Datenschutzgesichtspunkten ist es bedenklich, die Regelungen des Gesetzes zu Art. 10 GG uneingeschränkt anzuwenden.

6.4 Für die in den zentralen Einrichtungen der Neuen Medien beschäftigten Bediensteten ist ein Zeugnisverweigerungsrecht und für alle dort gespeicherten Daten ein Beschlagnahmeverbot (vgl. § 97 StPO) zu verlangen.

7. Datenschutzkontrolle und Datensicherung

7.1 Die Kontrolle des Datenschutzes bei Neuen Medien sollte Aufgabe der Datenschutzbeauftragten des Bundes und der Länder sein.

7.2 Beim Anschluß von EDV-Einrichtungen durch Teilnehmer sind hinreichende technische und organisatorische Maßnahmen zu fordern, sowohl hardware- als auch softwaremäßig, z. B. Schlüsselschalter, Paßwortroutinen usw.

3.9.5 Erforderlichkeit eines Gesetzes?

In Bayern wird derzeit noch geprüft, inwieweit bereits zur Durchführung des Pilotprojektes in München ein Gesetz erforderlich ist. Der Landtag Rheinland-Pfalz hat mit Beschluß vom 27. 11. 1980 ein „Landesgesetz über einen Versuch mit Breitbandkabel“ beschlossen, das erfreulicherweise einige Datenschutzforderungen berücksichtigt. Für die Versuche mit Bildschirmtext bestehen in den Ländern Berlin und Nordrhein-Westfalen jeweils Gesetze (BerlGVBl S. 1002 Gesetz v. 29. 5. 1980; GVBl NW S. 153, Gesetz v. 18. 3. 1980; VO über Beginn und Dauer des Feldversuches vom 25. 3. 1980, GVBl NW S. 258).

In die entsprechenden Überlegungen in Bayern werden folgende Gesichtspunkte einbezogen werden müssen: Soweit für den bayerischen Feldversuch das Bayerische Datenschutzgesetz einschlägig ist, ist zu berücksichtigen, daß nach dem 1. 1. 1983 Speicherung, Veränderung und Übermittlung von Daten nur noch zur rechtmäßigen Erfüllung der durch Rechtsnorm zugewiesenen Ausgaben zulässig sind. Für die im Rahmen von Teilnehmerbefragungen erforderlichen Datenerhebungen dürfte sich die Schaffung einer Rechtsgrundlage empfehlen, wenn die entsprechenden Angaben von allen Teilnehmern erwartet werden. Andernfalls müßten die Teilnehmer nach Art. 16 Abs. 2 BayDSG auf die Freiwilligkeit der Angabe von Daten hingewiesen werden. Die erforderlichen Verbote bestimmter Nutzungsarten, z. B. die allenfalls nur beschränkte Nutzung des Rückkanals, dürften auf gesetzlicher Grundlage nachhaltiger durchgesetzt werden können. Auch der im Bereich der Neuen Medien dringend erforderliche bereichsspezifische Datenschutz könnte aufgrund eines Gesetzes bereits in der Pilotphase, soweit für diese erforderlich, verankert werden. In diesem Zusammenhang weise ich darauf hin, daß meines Erachtens die Speicherung oder anderweitige Verarbeitung z. B. von Teilnehmerdaten, die zum Zwecke der Verwaltung, Kontrolle oder Analyse von Kommunikationsvorgängen betrieben werden, nicht unter das Medienprivileg fallen. Selbst wenn für einige Angebote der Neuen Medien der Rundfunkbegriff anzuwenden ist, fallen derartige Daten nur mittelbar bei publizistischer Tätigkeit an und dienen somit nicht ausschließlich publizistischen Zwecken. Um die Beachtung der dem Datenschutz dienenden Bestimmungen durchsetzen zu können, erscheinen Bußgeldvorschriften sinnvoll. Diese könnten nur auf Grundlage einer entsprechenden Rechtsnorm vorgesehen werden. Schließlich könnte es sich zur Klarstellung empfehlen, die Datenschutzaufsichtsinstanz über die Betreiber des Pilotprojektes gesetzlich eindeutig festzulegen.

Sollten die Beratungen der Projektkommission „Neue Medien“ ergeben, daß es zur Durchführung des Kabelpilotprojektes in München einer gesetzlichen Regelung nicht bedarf, wird zu prüfen sein, ob die Datenschutzforderungen ausreichend auf nichtgesetzlichem Wege erfüllt werden können.

3.10 Verschiedenes

3.10.1 Lichtbilder

Von verschiedenen Stellen und in einer Eingabe bin ich zum Umgang mit Lichtbildern befragt worden, die sich im Besitz von Behörden befinden. Da sich das Recht am eigenen Bild – soweit überhaupt geschützt ist – aus dem allgemeinen Persönlichkeitsrecht der Art. 1 und 2 Grundgesetz herleitet, sei kurz über hier bekanntgewordene Fälle berichtet:

- Das Paßamt einer Gemeinde wurde gebeten, aus der Personalausweiskartei das Lichtbild einer Person zu Illustrierung eines Beitrags in einer Tageszeitung zur Verfügung zu stellen.
- Reporter verlangten bei einer Gemeinde nach Lichtbildern bis dahin der Öffentlichkeit nicht bekannter Personen, die im Zuge einer aufsehenerregenden Affäre Selbstmord begangen hatten.

Das Kunsturhebergesetz ist hier anzuwenden (Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie vom 9. 1. 1907, BGBl. III 440/3, zuletzt geändert durch Gesetz vom 2. 3. 1974, BGBl. I S. 469). Danach dürfen Lichtbilder grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder veröffentlicht werden. § 24 des Gesetzes läßt die Weitergabe und Veröffentlichung von Lichtbildern durch Behörden, beschränkt auf „Zwecke der Rechtspflege und öffentlichen Sicherheit“ zu. Beide Fälle waren nicht gegeben. Nach § 22 darf die Gemeinde aus ihren Unterlagen Bilder von Verstorbenen bis zum Ablauf von 10 Jahren nach dem Tod nur mit Einwilligung der Angehörigen des Abgebildeten an Dritte zur Verfügung stellen. Ausnahmefälle nach § 23 des Kunsturhebergesetzes (Bildnisse aus dem Bereich der Zeitgeschichte, Bilder von Versammlungen u. ä.) waren in den vorgelegten Fällen nicht erkennbar. Das Bayer. Staatsministerium des Innern hat in einem solchen Fall festgestellt, daß ein für die Ausstellung von Ausweisen der Gemeinde ausgehändigtes Bild nicht dadurch ein „Bildnis aus dem Bereich der Zeitgeschichte“ werde, daß die abgebildete Person sich im Zusammenhang mit einem gegen sie gerichteten Ermittlungsverfahren das Leben nimmt.

3.10.2 Öffentliche Zustellungen aufgrund des Bayer. Verwaltungszustellungs- und Vollstreckungsgesetzes

Bei der öffentlichen Zustellung von Schriftstücken stellt sich die Frage, welche personenbezogenen Angaben durch die öffentliche Form der Zustellung Dritten ohne Verletzung des Persönlichkeitsrechts des Betroffenen bekanntgegeben werden dürfen. Öffentliche Zustellungen können nicht nur in solchen Fällen in Betracht kommen, in denen der Zustellungsempfänger bewußt seinen Aufenthalt verheimlicht, sondern z. B. auch in Fällen, in denen der Betroffene

nach länger zurückliegendem Wegzug nicht mehr erreichbar ist. Die Frage nach der „Schutzwürdigkeit“ möglicherweise beeinträchtigter Belange ist deshalb nicht einheitlich zu beantworten.

Bei den öffentlichen Zustellungen gemäß Art. 15 des Bayer. Verwaltungszustellungs- und Vollstreckungsgesetzes war seit jeher der Datenschutz zu berücksichtigen. Besondere Geheimhaltungsvorschriften z. B. Sozialgeheimnis, Geheimhaltung von Patientendaten usw.) waren schon bisher von den zuständigen Behörde zu beachten, so daß bei der öffentlichen Zustellung unterschieden werden mußte, ob das Schriftstück als solches, oder nur eine entsprechende neutrale Benachrichtigung auszuhängen war (Art. 15 Abs. 2 Satz 2 VWZVG).

Nach dieser „sonstigen Datenschutzvorschrift“ kann in manchen Fällen das Aushängen des erlassenen Bescheides im vollen Wortlaut unzulässig sein.

3.10.3 Datengeheimnis — sonstige Nutzung von Daten

Art. 14 Abs. 1 BayDSG und § 5 Abs. 1 BDSG verpflichten die bei der Datenverarbeitung in öffentlichen Stellen beschäftigten Personen zur Einhaltung des Datengeheimnisses. Danach ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.

Ein Kontrollfall im Berichtsjahr hat ein Beispiel für den Fall einer „sonstigen Nutzung“ gegeben: Eine öffentliche Stelle erhielt von Bürgern deren Anschriften, um sie zur Erfüllung einer bestimmten Aufgabe nach einiger Zeit wieder anschreiben zu können. Ein Betroffener beschwerte sich beim Landesbeauftragten für den Datenschutz darüber, daß der zuständige Bedienstete der öffentlichen Stelle die Anschriften dazu benutzt habe, die Betroffenen in einer gänzlich anderen Angelegenheit anzuschreiben, deren Zugehörigkeit zu den Aufgaben dieses Bediensteten in der Eingabe außerdem bestritten wurde.

Eine Datenübermittlung i. S. d. BayDSG ist bei der Verwendung von Adressen gegenüber den Betroffenen selbst nicht gegeben (Art. 5 Abs. [2] Nr. 2 und Abs. 3 Nr. 2 BayDSG). Auch andere im Gesetz genannte Phasen der Datenverarbeitung liegen nicht vor. Zu prüfen war daher, ob diese — im Sinne des Datenschutzrechts — „sonstige Nutzung“ zu einer anderen als einer rechtmäßigen Aufgabe unbefugt erfolgte.

3.10.4 Auskunftsverweigerung „aus Gründen des Datenschutzes“

Öffentliche Stellen neigen, wie ich beobachte, gelegentlich dazu, von ihnen erbetene Auskünfte unter Berufung auf den Datenschutz zu verweigern, auch wenn weder das Datenschutzgesetz noch eine sonstige Verschwiegenheitspflicht dies veranlaßt. Es ist zwar unbestritten, daß die Abgrenzung des Datenschutzrechts in der Praxis Schwierigkeiten bereitet, es ist aber dem Datenschutz abträglich, wenn er zur Begründung von Ablehnungen in Anspruch genommen wird, die mit ihm nichts zu tun haben.

So verweigerte eine Gemeinde die Auskunft über die Lage des Grabes einer bestimmten Person auf dem gemeindlichen Friedhof mit Hinweis auf den Datenschutz. Derartige Antworten stoßen deshalb auf Unverständnis in der Bevölkerung.

3.10.5 Tätigkeit von Kommunalbediensteten für Kreditauskunfteien

Es haben sich Anhaltspunkte dafür ergeben, daß vereinzelt Bedienstete von Gemeinden „außerhalb des Dienstes“ Fragebogen von Kreditauskunfteien über Gemeindebürger ausfüllen. Ich halte es zumindest aus allgemeinen datenschutzrechtlichen Erwägungen für bedenklich, wenn Mitarbeiter von Gemeindeverwaltungen oder Verwaltungsgemeinschaften gleichzeitig als Vertrauensleute für Kreditschutzeinrichtungen tätig sind, da die weitergegebenen Informationen den Bediensteten i. d. R. nur deshalb bekannt sind, weil sie auf Grund ihrer Beschäftigung in der Gemeinde oder Verwaltungsgemeinschaft auch — über amtlich erhobene Daten hinaus — Kenntnisse über die „persönlichen oder sachlichen Verhältnisse“ von Einwohnern haben.

Das Bayer. Staatsministerium des Innern, dem ich meine Bedenken mitgeteilt hatte, hat mit Schreiben vom 7. Oktober 1980 Nr. I A 7 - 480 - 5/57 über die Regierungen und Landratsämter die Gemeinden gebeten, Genehmigungen für derartige Nebentätigkeiten zu versagen.

3.11 Allgemeine Feststellungen zur Kontrolltätigkeit im Bereich der technischen und organisatorischen Maßnahmen (Art. 15 BayDSG)

Im 2. Tätigkeitsbericht wurde unter Nr. 2.2 über die ersten Kontrollen der Datensicherungsmaßnahmen in Rechenzentren berichtet.

Im Berichtszeitraum wurden 6 Großrechenzentren der öffentlichen Verwaltung überprüft. Es handelte sich dabei um 2 kommunale Rechenzentren, 3 staatliche Rechenzentren und um 1 Rechenzentrum aus dem Bereich der Allgemeinen Ortskrankenkassen.

Darüber hinaus wurden im Rahmen dieser Prüfungen auch einige an diese Rechenzentren angeschlossene Fachdienststellen überprüft. Es hat sich nämlich gezeigt, daß die Datensicherungsmaßnahmen in Großrechenzentren in zunehmendem Maße den Anforderungen des Datenschutzes entsprechen, Mängel bei den organisatorischen Maßnahmen zur Datensicherung jedoch bei den datenverarbeitenden Fachdienststellen selbst auftreten, etwa bei kommunalen Fachämtern, Landratsämtern oder Universitätskliniken.

Schließlich wurde im Berichtszeitraum damit begonnen, auch kleinere Gemeinden und Landratsämter zu besuchen, um dort die bei den ADV-Einrichtungen getroffenen technischen Maßnahmen der Datensicherung sowie die organisatorischen Maßnahmen zur Datensicherung bei manuell geführten Dateien (Karteien) zu überprüfen. Insgesamt wurden dabei 40 Stellen besucht: 29 kreisangehörige Gemeinden, Verwaltungsgemeinschaften oder Städte in den Landkreisen Altötting, Mühldorf, Passau, Rosenheim und Traunstein, die Landratsämter Mühldorf am Inn, Pas-

sau, Traunstein und Würzburg, die kreisfreie Stadt Passau sowie die Stadtwerke Passau, ein Kreiskrankenhaus, eine Studentenkanzlei einer Fachhochschule und zwei Polizeiaußenstellen.

Bevor ich auf Mängel im einzelnen näher eingehe, kann ich erfreulicherweise berichten, daß die von meinen Mitarbeitern überprüften Stellen selbst die Ergebnisse der Überprüfungen offenbar an andere Stellen weitergeben, so daß bei deren Kontrolle Mängel gleicher Art zunehmend seltener auftraten. So gab der Landesverband der Ortskrankenkassen in Bayern die Erkenntnisse der ersten Prüfung in einem AOK-Rechenzentrum im Jahre 1979 dem nachgeordneten Bereich bekannt. Bei der im Berichtszeitraum durchgeführten Kontrolle eines weiteren AOK-Rechenzentrums traten Verstöße gegen Datenschutzbestimmungen, wie sie ein Jahr vorher festgestellt worden waren, im wesentlichen nicht mehr auf. Auch bei den besuchten Allgemeinen Ortskrankenkassen zeigte es sich, daß die an anderer Stelle gewonnenen Erfahrungen bereits ausgewertet waren und einige Kassen bereits umfangreiche und wirkungsvolle Datensicherungsmaßnahmen veranlaßt hatten.

3.11.1 Prüfung der technischen und organisatorischen Datensicherungsmaßnahmen in Rechenzentren

Die unter Nr. 2.2.2 im Tätigkeitsbericht des Jahres 1979 aufgeführten Mängel in Rechenzentren wurden auch bei den im Berichtszeitraum durchgeführten Kontrollen festgestellt. Die meisten Beanstandungen traten in folgenden Bereichen auf:

- Fehlende Abschottung des inneren Sicherheitsbereiches im Rechenzentrum (Zugangskontrolle);
- Fehlen einer wirkungsvollen Datenträgerverwaltung im Archiv; in den meisten Fällen kann nicht festgestellt werden, wo sich gegenwärtig welche maschinell lesbaren Datenträger befinden (Abgangskontrolle);
- Fehlen eines wirksamen Zugriffsschutzes auf Dateien (Zugriffskontrolle);
- Fehlen einer Möglichkeit, die ordnungsgemäße Anwendung von Dienstprogrammen zu kontrollieren;
- keine Trennung von Test- und Produktionsbetrieb.

Gute Dienste bei der Festlegung der notwendigen Maßnahmen zur Datensicherung leistete dabei der „Katalog der technischen und organisatorischen Maßnahmen zum Datenschutz“ (siehe dazu im 2. Tätigkeitsbericht unter 3.2). Dieser Katalog, den eine Arbeitsgruppe des Staatlichen Koordinierungsausschusses Datenverarbeitung zusammengestellt hatte, wurde von diesem Koordinierungsausschuß am 30. 7. 1980 gebilligt und seine Anwendung in den Rechenzentren der staatlichen Verwaltung empfohlen. Bei seiner Anwendung wurde darauf geachtet, daß die geforderten Maßnahmen in einem angemessenen Aufwand zum Schutzzweck stehen. Der Katalog soll der Verwaltung in erster Linie als Richtschnur zur Festlegung von Datensicherungsmaßnahmen und meiner Dienststelle als Anhalt zu einer möglichst objektiven Bewertung gleicher Sachverhalte dienen.

Als Beispiel für die Organisation des inneren Sicherheitsbereiches eines Rechenzentrums möchte ich an dieser Stelle Forderungen aufzeigen, die an den Betrieb eines überprüften Rechenzentrums gestellt wurden. Für die Zugangs- und Abgangskontrolle im inneren Sicherheitsbereich wurden folgende Forderungen erhoben:

- Verschließbarkeit der einzelnen Räume, Anbringen elektrischer Türöffner und -schließer;
- Kontrolle der Zugangsberechtigten über ein Ausweisesystem;
- Sicherung des gesamten inneren Sicherheitsbereiches außerhalb der Arbeitszeit (ein Bewegungsmelder genügt in der Regel den Anforderungen nicht, wenn er nicht den gesamten inneren Sicherheitsbereich erfaßt);
- räumliche Trennung von Bediennraum, Archiv, Arbeitsvor- und Arbeitsnachbereitung;
- Verbesserung der Fenstersicherung;
- Anschluß der Räume, in denen EDV-Geräte untergebracht sind, an das Sicherungssystem;
- Unterbringung des Wartungspersonals außerhalb des inneren Sicherheitsbereiches;
- Einführung eines Schalterbetriebs zur Übernahme der Aufträge von Benutzern sowie zur Übergabe der Ergebnisse an die Benutzer (für besonders sensible Auswertungen Schließfächer);
- ein Raum außerhalb des Sicherheitsbereiches für Taschen und Garderobe für Bedienstete, die ihren Arbeitsplatz im inneren Sicherheitsbereich haben.

Ich darf in diesem Zusammenhang ausdrücklich betonen, daß die Mehrzahl der besuchten Rechenzentren den Anforderungen des Datenschutzes im großen und ganzen genügte.

3.11.2 Datensicherungsmaßnahmen bei Universitätskliniken

Im Klinikbereich wurden neben den Dateien, die in einem automatisierten Verfahren verarbeitet werden, auch die manuellen Karteien und Krankengeschichten in die Kontrolle mit einbezogen. Für die Aufbewahrung dieser Dateien mit personenbezogenen Daten habe ich u. a. folgende Forderungen gestellt:

- Für die Aufbewahrung der Karteien und Krankengeschichten sind grundsätzlich verschließbare Behältnisse erforderlich. Bei Räumen, in denen personenbezogene Daten aufbewahrt werden, ist darauf zu achten, daß außerhalb der Dienstzeit und zu den Zeiten, in denen sie nicht besetzt sind, Unbefugten die Kenntnisnahme dieser Daten nicht möglich ist. Es ist deshalb u. a. auch erforderlich, daß diese Räume während der Dienstzeit gereinigt werden, so daß das Vier-Augen-Prinzip gewahrt wird.
- Sofern eine Unterbringung der Dateien in verschließbaren Schränken nicht möglich ist, ist dafür zu sorgen, daß die Räume, in denen sie sich befinden, nur von Befugten betreten werden können.
- Der Transport von Krankengeschichten vom behandelnden Arzt zum Archiv und zurück darf nicht offen

erfolgen. Umlaufende Krankengeschichten müssen nach Dienstschluß stets unter Verschuß gehalten werden.

Im übrigen sei auf die in Art. 13 Abs. 4 Bayer. Krankenhausgesetz (BayKHG) vorgezeichnete Trennung von Verwaltungsdaten und medizinischen Daten im Krankenhaus hingewiesen.

3.11.3 Prüfung der technischen und organisatorischen Sicherungsmaßnahmen bei Kommunalbehörden

Wie erwähnt, wurden im Berichtszeitraum die technischen und organisatorischen Datensicherungsmaßnahmen bei insgesamt 30 Gemeinden, Verwaltungsgemeinschaften, Städten bzw. kreisfreien Städten überprüft. Die häufigsten Mängel, die sich bei diesen Kontrollbesuchen, die in erster Linie den Charakter einer Beratung hatten, ergaben, betrafen

- die Zugangssicherung,
- die Aufbewahrung von maschinell lesbaren Datenträgern, Karteikarten oder Listen,
- die Vernichtung von nicht mehr benützbaren maschinell lesbaren Datenträgern und nicht mehr benötigten Karteikarten.

Darüber hinaus war in vielen Fällen die Nichtbeachtung der Meldepflicht zum Datenschutzregister und ein Fehlen der Verpflichtung der in der automatisierten Datenverarbeitung Beschäftigten auf das Datengeheimnis festzustellen. Im übrigen war eine Zuständigkeit für Datenschutzangelegenheiten lediglich bei 5 Stellen in der Geschäftsverteilung geregelt.

Im übrigen wurde angeregt, ein Verzeichnis über alle automatisiert und manuell verwalteten Dateien zu führen. Den Stellen wurde zusammen mit dem Schlußbericht ein Formblattmuster für manuell verwaltete Karteien zugeleitet. Die Karteierhebung soll dem für Datenschutzangelegenheiten Zuständigen einen Überblick über die (auch) dem Datenschutzgesetz unterliegenden manuellen Karteien geben. Folgende Informationen sollten mindestens erhoben werden:

- Zuständige Stelle;
- Karteibezeichnung, Karteinhalt, Speicherungszweck (mit Rechtsgrundlage), betroffener Personenkreis, Zahl der Fälle;
- regelmäßige Datenübermittlungen (Empfänger, Art der Daten, Rechtsgrundlage, Art der Übermittlung und Periodizität).

Darüber hinaus wurde empfohlen, in einer Dienstweisung für die technischen und organisatorischen Maßnahmen der Datensicherung insbesondere folgende Arbeitsschritte zu regeln:

- Anlegen und Bearbeiten von Dateien;
- Weitergabe von Daten (Übermittlung und Transport);
- Aufbewahrung der Dateien;
- Vernichten von Dateien.

3.11.4 Prüfung der technischen und organisatorischen Datensicherungsmaßnahmen bei Landratsämtern

Im Berichtszeitraum wurden, wie bereits erwähnt, vier Landratsämter besucht. Soweit die personelle Zuständigkeit für Datenschutzangelegenheiten bereits geregelt war, entsprachen im großen und ganzen die Datensicherungsmaßnahmen den Vorschriften des Datenschutzes. Die besuchten Landratsämter sind über eine Datenstation an Rechner der Anstalt für Kommunale Datenverarbeitung angeschlossen und wickeln dort eine Reihe von Aufgaben automatisiert ab. Darüber hinaus werden an diesen Datenstationen zum Teil auch Erfassungsarbeiten für Gemeinden des Landkreises erledigt.

Für den Beleg austausch von der Fachabteilung zu der Stelle, die die Daten maschinell erfaßt und an den Großrechner übermittelt, habe ich verschlossene Mappen gefordert.

Wegen des Aufgabenumfanges der Landratsämter ist es dort besonders nützlich, wenn der Datenschutzbeauftragte des Landratsamtes ein Verzeichnis über alle in diesem Amt automatisiert und manuell verwalteten Dateien führt.

Um die Arbeit der Aufsichtsbehörden und meine Arbeit zu erleichtern, habe ich außerdem angeregt, in den Landratsämtern eine Übersicht darüber anzulegen, welche Gemeinden welche Aufgaben an welcher ADV-Anlage abwickeln oder bei welcher Stelle im Auftrag abwickeln lassen. Die Erfahrungen haben im übrigen auch gezeigt, daß eine Vielzahl von Gemeinden Kleincomputer besitzt, ohne bisher ihrer Meldepflicht nach § 7 der Datenschutzregisterverordnung nachgekommen zu sein.

3.11.5 Prüfung der organisatorischen Datensicherungsmaßnahmen einer Studentenkanzlei einer Fachhochschule

Im Zusammenhang mit der Überprüfung von Datenübermittlungen aus der Studentenkartei einer Fachhochschule wurde die Unterbringung der allgemeinen Studentenkartei und der Meldekartei, in der dortigen Studentenkanzlei kontrolliert. Da beide Karteien zum Teil recht sensible Daten enthalten, sind bei der Aufbewahrung angemessene Sicherungsmaßnahmen erforderlich.

Da die Karteien zum Teil offen auf den Arbeitstischen oder in nicht absperrbaren Schränken standen und die Studentenkanzlei außerhalb der Dienstzeit auch Bediensteten anderer Abteilungen zugänglich war, habe ich die bisherige Handhabung beanstandet und gefordert, die Studentendaten gesichert aufzubewahren und dem Datenschutz mehr Bedeutung beizumessen. Auch bei unzulänglicher räumlicher Unterbringung müssen Karteien mit sensiblen Daten zuverlässig verwahrt werden.

3.11.6 Grundsätze für die Verarbeitung von Dateien mit personenbezogenen Daten

Alle speichernden Stellen, die personenbezogene Daten in einem automatisierten Verfahren verarbeiten, sollten die Datensicherungsmaßnahmen für alle Ein-

zelschritte so regeln, daß Sinn und Zweck jeder Einzelmaßnahme klar erkennbar wird. Eine Dienstanweisung über Datensicherungsmaßnahmen bei der Verarbeitung von automatisiert geführten Dateien sollte insbesondere folgende Arbeitsgänge regeln:

- Zugang zu den Räumen, in denen die Geräte aufgestellt sind,
- Zutrittsbefugnisse außerhalb der Dienstzeit,
- Befugnis zur Bedienung der EDV-Geräte,
- Aufbewahrung der Bedienungshandbücher,
- Erfassung von Daten,
- Transport, Aufbewahrung und Rückgabe der Datenerfassungsbelege,
- Auftrags erledigung,
- Anfertigung von Sonderauswertungen (Dokumentation),
- Verteilung der Ergebnisse und Auswertungen an die Fachabteilung,
- Aufbewahrung maschinell lesbarer Datenträger,
- Vernichtung von Datenträgern und fehlerhaften Auswertungen.

Weiter ist darauf zu achten, daß nur die im Rahmen der Aufgabenerledigung erforderlichen personenbezogenen Daten gespeichert, verändert und übermittelt werden. Werden auf ADV-Anlagen eigene Verfahren entwickelt, ist darauf zu achten, daß für Testzwecke nur solche Daten verwendet werden, die keinen Rückschluß auf eine bestimmte Person zu lassen.

Im übrigen kommt der Lage der Räume, in denen ADV-Geräte aufgestellt sind, besondere Bedeutung zu. Eine Reihe von Beanstandungen beruht auf unzureichenden baulichen Gegebenheiten. Die Planung für den Bau von Rechenzentren erfolgte häufig zu einer Zeit, in der Datenschutz noch wenig Beachtung fand. Im Berichtszeitraum wurde ich auf Ersuchen einiger Stellen mehrmals bei Neubaumaßnahmen beratend tätig.

Da es nicht möglich ist, allgemeine Aussagen über die in jedem Einzelfall dem Schutzzweck angemessenen notwendigen Datensicherungsmaßnahmen zu machen, empfehle ich, sich zunächst an den im sog. Datensicherungskatalog des Staatl. Koordinierungsausschusses Bayern aufgeführten Einzelmaßnahmen zu orientieren. In schwierigen Fällen stehen meine Mitarbeiter beratend zur Verfügung.

Im übrigen sollte, soweit es die Größe einer Behörde zweckmäßig erscheinen läßt, ein Bediensteter für Datenschutzangelegenheiten zuständig sein und einen Überblick über alle Datenspeicherungen und Datenübermittlungen (Dateierhebung) besitzen. Schließlich sollte sich der für den Datenschutz Zuständige durch gelegentliche Kontrollen von der Einhaltung der angeordneten Datensicherungsmaßnahmen überzeugen.

3.11.7 Überlegungen zur ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen

Wie bereits im letzten Tätigkeitsbericht unter der Nummer 2.2.4 berichtet, erstellte eine Arbeitsgruppe

von Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und Datenschutzbeauftragten unter der Federführung des Bayer. Landesbeauftragten für den Datenschutz ein Papier, das Kriterien und Regeln enthält, die betrieblichen wie behördlichen Datenschutzbeauftragten die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme erleichtern sollen. Die Zusammenstellung beschreibt in einem Teil A den Rahmen sinnvoller Kriterien zur Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen. Teil B enthält Anforderungen, ohne deren Erfüllung eine ordnungsgemäße Anwendung der Datenverarbeitungsprogramme im öffentlichen Bereich grundsätzlich nicht möglich ist.

Für den Bereich der Programmierung wurden aus der Sicht des Datenschutzes Regeln für die Organisation der Programmierabteilung, für die Programm-erstellung und -pflege, für die Programmdokumentation sowie für programmtechnische Kontrollen gegeben. Die Beachtung dieser Regeln erleichtert es dem für den Datenschutz Zuständigen, den ordnungsgemäßen Ablauf der Datenverarbeitungsprogramme zu überprüfen.

Bei der Organisation der Programmierung sind grundsätzlich die geltenden Programmier- und Dokumentationsregeln zu beachten. Abweichungen sind zu begründen und zu dokumentieren. Im einzelnen gelten folgende Regeln:

- Einhaltung der Programmier- und Dokumentationsanweisungen,
- Closed-Shop-Betrieb auch während der Programmierphase,
- zusätzliche Maßnahmen für die interaktive Programmierung,
- Erstellung signifikanter Testdateien.

3.12 Technische Einzelfragen

3.12.1 Temporäre Dateien

Datensicherungsmaßnahmen nach Art. 15 Abs. 2 Bayer. Datenschutzgesetz gelten für jede physische Datei, die in einem automatisierten Verfahren gespeichert wird, also auch für sogenannte „temporäre Dateien“, die nur kurzzeitig existent sind. In der Regel enthalten diese temporären Dateien keine Informationen, die nicht auch in einem Stammdatenbestand enthalten sind. Freilich ist auch denkbar, daß in temporären Dateien Zusatzinformationen gespeichert werden. Solche zusätzlichen Datenarten wären grundsätzlich in die Datenbeschreibung der Meldung zum Datenschutzregister mit aufzunehmen. In der Praxis dürfte dieser Fall nur selten vorkommen. Allgemein ist festzustellen, daß „temporäre Dateien“ nur spezielle Ausprägungen der Stammdateien ohne Zusatzinformationen sind und nach dem Datenschutzgesetz denselben Maßnahmen zur Datensicherung nach Art. 15 Abs. 2 BayDSG unterliegen wie die Stammdateien.

Schwieriger ist die Behandlung von solchen Dateien, die entweder logisch oder physisch nur eine kurze Zeit existieren, sog. „kurzlebige Dateien“.

Hier kann man zwei Fälle unterscheiden:

1. Ist eine logische Datei kurzlebig, z. B. wenn sie für eine bestimmte, zeitlich begrenzte Aufgabe Daten angelegt ist, gilt: Eine solche Datei unterliegt dem Datenschutzgesetz; im Gesetz ist über die Lebensdauer einer Datei nichts ausgesagt. Eine Meldung zum Datenschutzregister kann sich aber im Einzelfall wegen der nur kurzen Speicherdauer erübrigen. Der behördliche Datenschutzbeauftragte sollte von der Existenz solcher Dateien Kenntnis haben. Bei Auskunftersuchen muß, sofern die Datei zu diesem Zeitpunkt gerade existiert, Auskunft an den Betroffenen erteilt werden.

2. Der Inhalt einer Datei ist kurzlebig:

Ein Beispiel können Adreßdateien mit wechselndem Inhalt sein, wobei nach Abwicklung der Aufgaben sämtliche Daten in der Datei physisch gelöscht werden. Die Datei unterliegt dem Datenschutzgesetz. Für das Konzept und die logische Datei ist nach Art. 7 BayDSG eine Meldung zum Datenschutzregister abzugeben. Es ist hier unerheblich, ob die logische Datei Daten enthält oder „leer“ (physisch gelöscht) ist. Im letzteren Fall wird auf ein Auskunftersuchen die Antwort „keine Daten gespeichert“ gegeben.

3.12.2 Datenschutzgerechte Papier- und Aktenvernichtung

Auf meine Anregung hat der staatliche Koordinierungsausschuß Datenverarbeitung die Frage der Vernichtung von Computerausdrucken usw. mit personenbezogenen Daten beraten. Nach einer Umfrage im staatlichen Bereich kam der Ausschuß zu dem Ergebnis, daß es zweckmäßig sei, das auszusondernde und zu vernichtende Schriftgut möglichst am Ort des Anfalls durch geeignete Geräte zu zerkleinern und an Abnehmer zur Weiterverwertung abzugeben. Eine zentrale Zerkleinerungsanlage wurde nicht für erforderlich gehalten.

Die Entscheidung deckt sich mit der Erkenntnis aus den Prüfungen der technischen und organisatorischen Maßnahmen zur Datensicherung in Großrechenzentren. Eine Vernichtung des auszusondernden Guts am Ort des Anfalls bringt weniger Gefahren und Datensicherungsprobleme mit sich.

3.12.3 Anforderungen an ein rechnergesteuertes Zugangskontrollsystem

Bei den heute gebräuchlichen Ausweislesesystemen für die Zugangskontrolle gibt es im wesentlichen zwei unterschiedliche Verfahren zur Erstellung der Ausweiskarten, das magnetisch aktiv-codierte Magnetstreifensystem und das induktiv-codierte System.

Vielfach wird die Auffassung vertreten, daß die induktive Codierung sicherer sei als die magnetisch aktive Codierung; die magnetisch aktive Codierung wird wegen der leichteren Manipulierbarkeit der aufgezeichneten Information als nicht genügend fälschungssicher angesehen. Bei der induktiven Codierung gilt es dagegen als nahezu ausgeschlossen, Ausweise zu fälschen.

Meines Erachtens ist aber nicht allein die Aufzeichnungsmethode als Kriterium für die Leistungsfähigkeit heranzuziehen. Wesentlich erscheint auch

- die Möglichkeit, unterschiedliche Raum- und Zeit-zonen definieren und bestimmte Personen suchen zu können;
- die Unterscheidung zwischen Zugang und Abgang sowie die Überprüfung der Paarigkeit;
- ein Alarm bei unberechtigten Zugangsversuchen;
- die Überwachung und Zeitsteuerung der Türöffnungsdauer;
- die Protokollierung der Zu- und Abgänge sowie eine besondere Kennzeichnung von unbefugten Zugangsversuchen;
- die Auswertung der aufgezeichneten Daten durch Programme;
- eine problemlose Handhabung der Zuweisung und Sperrung von Ausweisnummern sowie der Änderung der Berechtigung;
- ein Betrieb als autonomes System (bei Defekt der Zentrale muß das Zugangskontrollsystem funktionsfähig bleiben);
- eine ständige Betriebsbereitschaft;
- eine Sicherung der aufgezeichneten Daten bei Netzausfall.

Schließlich ist darauf zu achten, daß nur die nötigste Information auf den Ausweis codiert wird. Darüber hinaus sollte der Ausweis ein neutrales Aussehen haben, so daß bei Verlust nicht erkennbar wird, bei welcher Behörde dieser Ausweis Verwendung findet.

3.13 Mitarbeit in ADV-Benutzer-Arbeitskreisen

3.13.1 Mitarbeit in der Benutzervereinigung SCOUT e.V.

Anwender von Siemens-Groß-EDV-Anlagen haben sich 1975 in der Benutzervereinigung SCOUT e.V. (Siemens-Computer-User-Team) zusammengeschlossen. Innerhalb dieser Benutzervereinigung wurden Arbeitskreise gebildet, die regelmäßigen Erfahrungsaustausch pflegen. Im Juni 1979 konstituierte sich auch eine Arbeitsgruppe „Datenschutz“, die seit Anfang 1980 von einem Angehörigen meiner Geschäftsstelle geleitet wird. Die Arbeitsgruppe tagt dreimal im Jahr. Sie zählt derzeit 19 Mitglieder, davon je 6 aus dem Behördenbereich und der Industrie, 5 aus dem Bereich Banken und Versicherungen, je 1 Vertreter aus den Bereichen Handel und Verlagswesen. Die Mitarbeit in dieser Arbeitsgruppe kommt, wie ich glaube, einem praxisnahen Datenschutz sehr zugute.

Die Arbeitsschwerpunkte der Arbeitsgruppe „Datenschutz“ in SCOUT liegen sowohl im technischen, wie auch im organisatorischen und rechtlichen Bereich. Vordringliche Probleme, die von der Arbeitsgruppe behandelt werden, sind zum Beispiel

- technische und organisatorische Probleme der Datensicherung (Art. 15 BayDSG, Anlage zu § 6 Bundesdatenschutzgesetz);

- ordnungsgemäße Anwendung von DV-Programmen nach § 29 Abs. 2 Bundesdatenschutzgesetz;
- Beurteilung von Standardsoftware aus der Sicht des Datenschutzes;
- datenschutzrechtliche Beurteilung der Fernwartung (Teleservice);
- Diskussion über angebotene Hardware aus der Sicht des Datenschutzes;
- neue Techniken.

Die Arbeitsgruppe formulierte im Sommer 1980 zwei Entwicklungsanträge für Siemens-Software-Komponenten: Der erste fordert die Realisierung eines „bildschirmorientierten, dialogfähigen Datenträgerarchivsystems“ (Abgangskontrolle), der zweite „die software-unterstützte Kontrolle unzulässiger Zugriffe auf paßwortgeschützte Dateien“ (Zugriffskontrolle).

3.13.2. Mitarbeit in der Benutzervereinigung GUIDE

Anwender von IBM-EDV-Anlagen haben sich in der Benutzervereinigung GUIDE zusammengeschlossen. Innerhalb dieser Benutzervereinigung wurde ein Arbeitskreis „Datenschutz/Datensicherheit“ gebildet, der regelmäßigen Erfahrungsaustausch pflegt und in dem ebenfalls ein Angehöriger meiner Geschäftsstelle mitwirkt. Die 44 Mitglieder vertreten nahezu alle Bereiche der Wirtschaft sowie verschiedene öffentliche Stellen.

Die Arbeitsschwerpunkte liegen auch hier im technischen, organisatorischen und rechtlichen Bereich. Es besteht folgende generelle Zielsetzung:

- Gegenseitige Unterstützung beim Aufbau der Datenschutzorganisation mit dem Schwerpunkt Datenverarbeitung,
- Erfahrungsaustausch über Funktionen und Implementierung mit für Datenschutz und Datensicherheit verwendbarer Software,
- Erfahrungsaustausch über die Datenschutzpraxis und die Interpretation von einschlägigen Gesetzen und Vorschriften.

Im Jahr 1980 wurden u. a. folgende Probleme behandelt:

- Erfahrungsaustausch über die praktische Durchführung von Datensicherungsmaßnahmen gemäß § 6 Bundesdatenschutzgesetz,
- Erarbeitung von Grundsätzen ordnungsgemäßer Datenverarbeitung bzw. Anwendung von DV-Programmen,
- Beurteilung von Hard- und Software aus der Sicht des Datenschutzes,
- Anforderungen an die Dokumentation von EDV-Systemen,
- Diskussion über Datenschutzprobleme in Zusammenhang mit der fernunterstützten Wartung von EDV-Anlagen,
- Diskussion über Datenschutzfragen in Zusammenhang mit den Neuen Medien (z. B. „Bildschirmtext“).

Die Mitarbeit in den beiden Arbeitskreisen trägt wesentlich dazu bei, anstehende Datenschutzprobleme, die nicht allein den öffentlichen Bereich betreffen, zu erkennen und Lösungen vorzubereiten.

4. Datenschutz beim Bayerischen Rundfunk

Das Bayerische Datenschutzgesetz hat in Art. 21 das Datenschutzrecht für den Bayerischen Rundfunk gesondert geregelt und hierbei das Modell des autonomen Datenschutzes gewählt. Für die Kontrolle der Einhaltung des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz bei der gesamten Tätigkeit des Bayerischen Rundfunks ist nicht der Landesbeauftragte für den Datenschutz zuständig, sondern ausschließlich der Datenschutzbeauftragte des Bayerischen Rundfunks. Dieser hat auch gemäß Art. 21 Abs. 3 Satz 5 BayDSG den Organen des Bayerischen Rundfunks jährlich einen Bericht über seine Tätigkeit zu erstatten, der auch dem Landesbeauftragten für den Datenschutz zu übersenden ist. Dieser Verpflichtung ist er mit Vorlage seines 2. Tätigkeitsberichtes für den Zeitraum vom 1. 1.—31. 12. 1980 nachgekommen.

Das aktuelle Datenschutzregister des Bayerischen Rundfunks, das der dortige Datenschutzbeauftragte gesondert von dem Register des Landesbeauftragten für den Datenschutz führt, ist im Bayerischen Staatsanzeiger 1981, Nr. 15, veröffentlicht. Es enthält zum Stichtag 31. 1. 1981 18 vom Bayerischen Rundfunk geführte Dateien. Der Datenschutzbeauftragte des Bayerischen Rundfunks berichtet, daß die ihm durch Art. 21 Abs. 3 Satz 2 BayDSG übertragene Überwachung des Datenschutzes bei der gesamten Tätigkeit der Anstalt den ständigen Kontakt mit allen Fachbereichen und Mitarbeitern des Hauses erforderlich mache, soweit diese sich mit der Verarbeitung personenbezogener Daten befassen und soweit bei diesen damit das Risiko einer potentiellen Verletzung des Datenschutzes besteht. Einer der Schwerpunkte der Tätigkeit des Datenschutzbeauftragten des BR war die allgemeine Informationstätigkeit über den Datenschutz für die Mitarbeiter des Bayerischen Rundfunks und dessen Personalrat sowie die Durchführung der Verpflichtung auf das Datengeheimnis bei den Mitarbeitern, die in automatisierten Verfahren der Datenverarbeitung beschäftigt sind. Die Verpflichtung ist bis auf einige Einzelfälle abgeschlossen. Dabei wurde gleichzeitig mit der zuständigen Personalabteilung ein Verfahren entwickelt, das gewährleistet, daß auch bei den neu eintretenden Mitarbeitern, die im Bereich der EDV arbeiten werden, automatisch die Verpflichtung auf das Datengeheimnis vorgenommen wird. In Gesprächen mit der Personalabteilung wurde auch der besondere Schutz von Mitarbeiterdaten und die Handhabung der Personalakten besprochen. Unterbringung und Ausgabe von Personalakten konnte deutlich verbessert werden.

Der Datenschutzbeauftragte des Bayerischen Rundfunks hat die Regelung des Datenschutzes für die in Bayern gelegenen Gemeinschaftseinrichtungen der Rundfunkanstalten überprüft. Alle Gemeinschaftseinrichtungen – Institut für Rundfunktechnik GmbH (IRT), Rundfunk-Betriebstechnik GmbH (RTB) und Schule für

Rundfunktechnik (SRT) – sind juristische Personen des Privatrechts und unterliegen daher den Vorschriften des Bundesdatenschutzgesetzes. Die Voraussetzung für die Bestellung eines eigenen Datenschutzbeauftragten sind gemäß § 28 Abs. 1 BDSG nur beim IRT erfüllt.

Der Datenschutzbeauftragte des BR berichtet auch, daß sich das datenschutzrechtliche Problem der Abführung von Gewerkschaftsbeiträgen durch den Bayerischen Rundfunk inzwischen als bundesweites Problem dargestellt habe. Er habe federführend für alle Rundfunkanstalten der Bundesrepublik die Verhandlungen mit der betreffenden Gewerkschaft geführt. Dabei wurde eine datenschutzrechtlich einwandfreie Lösung bei der Beitragsabrechnung dadurch erreicht, daß jedes Mitglied beim Eintritt in die betreffende Gewerkschaft unter ausdrücklichen Hinweis auf die Datenschutzbestimmungen seine Einwilligung in die entsprechende Datenübermittlungen erklärt. Damit wird der Vorschrift von Art. 4 Abs. 2 BayDSG Rechnung getragen. Im Bereich der freien Mitarbeiter sei bisher vierteljährlich der betreffenden Gewerkschaft das Einkommen des jeweiligen Mitarbeiters zum Beitragseinzug mitgeteilt worden. Auch hier seien alle betreffenden Gewerkschaftsmitglieder auf die Notwendigkeit einer Einwilligung hingewiesen worden. Diese Aktion habe dazu geführt, daß ca. ein Drittel der betroffenen freien Mitarbeiter diese Einwilligung nicht erteilt habe, so daß der Bayer. Rundfunk insoweit die Einkommensdaten an die Gewerkschaft nicht mehr übermittelt.

Bei einer Überprüfung der Praxis des Betriebsarztes bei dessen Behandlung von Gesundheitsdaten der Mitarbeiter habe sich ergeben, daß sämtliche Gesundheitsdaten in sogenannten Patientenakten gesammelt werden, die nicht unter den Dateibegriff fallen. Diese Gesundheitsdaten stammen insbesondere aus den Einstellungsuntersuchungen und aus freiwilligen Vorsorgeuntersuchungen. Eine Übermittlung gesundheitlicher Daten aus diesen Akten an Dritte findet grundsätzlich weder innerhalb noch außerhalb des Hauses statt. Der Personalabteilung wird aufgrund der Einstellungsuntersuchung lediglich die Eignung oder Nichteignung für die in Aussicht genommene Tätigkeit mitgeteilt. Besteht bei freiwilligen Vorsorgeuntersuchungen ausnahmsweise die Notwendigkeit – z. B. aus Gründen der Arbeitssicherheit –, die Personalabteilung in bestimmtem Umfang über die Diagnose zu informieren, so erklärt der Mitarbeiter hiermit sein Einverständnis. Ebenso wird bei der Mitteilung gewisser Untersuchungsergebnisse an den Hausarzt verfahren.

Der Datenschutzbeauftragte des Bayerischen Rundfunks stellte fest, daß er im Rahmen seiner Tätigkeit keinen Grund zu formellen Beanstandungen habe feststellen können. Soweit er Hinweise gegeben habe, hätten diese bei den zuständigen Stellen Beachtung gefunden. Im übrigen habe sich als ausreichend erwiesen, für die nähere Zukunft Maßnahmen zur Verbesserung des Datenschutzes zu empfehlen. Themen dieser Tätigkeit seien insbesondere gewesen:

- Ein Auskunftersuchen eines Mitarbeiters,
- der Austausch von Honorarangaben zwischen den Rundfunkanstalten,

- die betriebliche Telefondatenerfassung,
- die Einsichtnahme in Personalakten durch Rechnungshofprüfer,
- die Mitteilung von Betriebsrenten an Krankenkassen,
- das mit dem Auskunftsrecht nach Presserecht begründete Verlangen eines Journalisten auf Aushängung von Stellenplänen,
- die erhebliche Zunahme von Werbebriefen an Mitarbeiter des Bayerischen Rundfunks unter ihrer Dienstadresse,
- der Übergang des Pilotprojekts der Arbeitszeitbewirtschaftung durch EDV im Bereich der Fernsehproduktion in die normale Arbeitsphase.

Von den Aufgaben unmittelbar beim Bayerischen Rundfunk abgesehen, kommt dem Datenschutz bei der Gebühreneinzugsstelle der Rundfunkanstalten (GEZ) besondere Bedeutung zu. Die von den Landesrundfunkanstalten und dem ZDF getragene nicht rechtsfähige Verwaltungseinrichtung GEZ hatte zum 31. 12. 1980 einen Bestand von 23 323 023 Hörfunkteilnehmern und 21 189 806 Fernsehteilnehmern zu verwalten. Hieraus resultierten bei einem täglichen Posteingang von ca. 30 000 Vorgängen im Jahre 1980 113 606 000 Geschäftsvorfälle. Die GEZ führte 3 677 964 gebührenpflichtige und 247 482 gebührenbefreite Hörfunkteilnehmer des Bayerischen Rundfunks. Bei den Fernsehteilnehmern des BR waren 3 374 707 Teilnehmer gebührenpflichtig und 185 565 gebührenbefreit. Bereits aus diesem Gesichtspunkt der Quantität hielt es der Datenschutzbeauftragte des BR für angebracht, den Datenschutz bei der GEZ als einen Schwerpunkt der Tätigkeit der Rundfunk-Datenschutzbeauftragten anzusehen. Der Arbeitskreis Datenschutzbeauftragte hat deshalb von Anfang an darauf geachtet, daß die GEZ innerbetriebliche technische und organisatorische Vorkehrungen trifft, die einen Datenmißbrauch ausschließen. Die von der Geschäftsleitung der GEZ vorgenommenen technischen und organisatorischen Maßnahmen seien inzwischen mehreren Überprüfungen unterzogen worden. Soweit erforderlich, werde laufend an Verfahrensänderungen gearbeitet, die die Beachtung des Datenschutzes weiter absichern sollen.

Ein im Berichtszeitraum in einer Presseveröffentlichung enthaltener Hinweis über eine Rasterfahndung des Bundeskriminalamtes unter angeblicher Verwendung von Daten der GEZ von nicht-angemeldeten Rundfunkteilnehmern entsprach nicht den Tatsachen. Der GEZ stehen nur die Daten über angemeldete Rundfunkteilnehmer zur Verfügung. Eine Weitergabe solcher Daten an das BKA ist nicht erfolgt.

Im übrigen wurde im Rahmen der GEZ dem Datenschutz auch dadurch verstärkt Rechnung getragen, daß die für den Beauftragtendienst der Landesrundfunkanstalten von der GEZ auf Karten ausgedruckten Teilnehmerdaten erheblich reduziert wurden und die Mitteilung an den einzelnen Rundfunkteilnehmer über den Ablauf der Gebührenbefreiung statt als Postkarte, wie bisher, nun als Briefdrucksache versandt wird. Außerdem wird für Auskunftsverlangen

über gespeicherte Daten von Rundfunkteilnehmern keine Gebühr gefordert.

Der Datenschutzbeauftragte des Bayerischen Rundfunks weist in seinem Tätigkeitsbericht auch auf die Datenschutzproblematik der neuen Medien hin. Zwar lasse sich dieser Bereich derzeit noch nicht völlig übersehen, doch läge die Notwendigkeit datenschutzrechtlicher Maßnahmen auf der Hand. Selbst

bei einer zurückhaltenden Bewertung lasse sich feststellen, daß die bestehenden datenschutzrechtlichen Vorschriften den hier zu erhebenden Forderungen nicht entsprechen würden (s. a. Nr. 3.9.5. meines Tätigkeitsberichts).

Bezüglich weiterer Einzelheiten wird auf den Tätigkeitsbericht des Datenschutzbeauftragten des Bayerischen Rundfunks verwiesen.

Anhang 1

Rechtliche Grundlagen des Datenschutzes in Bayern

1.1 Vorschriften:

Für alle bayerischen Behörden gilt das Bayer. Datenschutzgesetz (BayDSG, BayGVBI 1978 S. 165).

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

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

Neben den Datenschutzgesetzen gelten eine Vielzahl von Gesetzen, die das Persönlichkeitsrecht bzw. einzelne Geheimnisse schützen. Als Beispiel seien § 35 des Sozialgesetzbuches (Sozialgeheimnis), § 203 StGB (u. a. ärztliche Schweigepflicht), § 30 Abgabenordnung (Steuergeheimnis) und Art. 30 des Bayer. Verwaltungsverfahrensgesetzes (Amtsverschwiegenheit) genannt. Außerdem gibt es spezielle Datenschutzvorschriften, wie Art. 13 des Bayer. Krankenhausgesetzes vom 21. Juli 1974 über die Behandlung von Patientendaten (GVBI S. 256), 1980 sind als sog. bereichsspezifische Datenschutzbestimmungen das Gesetz zur Änderung des Gesetzes über Personalausweise vom 6. 3. 1980 (BGBl I S. 270), das Melderechtsrahmengesetz vom 16. 8. 1980 (BGBl I S. 1429) sowie das Zehnte Buch Sozialgesetzbuch – SGB X – vom 18. 8. 1980 (BGBl I S. 1469) erlassen worden.

Solche spezielle Schutznormen gehen dem Bayerischen bzw. dem Bundesdatenschutzgesetz vor. BayDSG und BDSG sind Auffanggesetze, die einen Mindeststandard an Datenschutz gewährleisten. Der Gesetzgeber ist davon ausgegangen, daß besonders empfindliche Bereiche durch spezielle Datenschutzregelungen angemessener geregelt werden können und müssen.

Für die Anwendung des **BayDSG** sind folgende Ausführungsbestimmungen erlassen worden:

- Die Bekanntmachung zum **Vollzug des BayDSG** vom 12. 9. 1978 (MABI S. 688 ff.); ergänzt durch Bekanntmachung vom 4. 9. 1979 (MABI S. 527 und KMBI I 1980 S. 39).
- Die Bekanntmachung zum **Vollzug des BayDSG** vom 4. 9. 1979 (MABI S. 527), durch die die Vollzugsbekanntmachung zum BDSG vom 30. 1. 1979 (MABI S. 22) über die **Maßnahmen zur Datensicherung** für entsprechend anwendbar erklärt wurde (siehe auch KMBI I 1980 S. 39).
- Die Verordnung über das **Datenschutzregister** vom 23. 11. 1978 (Datenschutzregisterverordnung – DSRegV – GVBI S. 783). Sie legt den Inhalt des Datenschutzregisters fest, regelt die Einsicht in das Register, beschränkt die Meldepflicht der speichernden Stellen und bestimmt den Umfang der jährlichen Veröffentlichung aus dem Register.
- Die Kostenordnung für die Tätigkeit des **Technischen Überwachungsvereins Bayern e. V.** beim Vollzug der Da-

tenschutzgesetze vom 16. August 1979 (Datenschutzkostenordnung – DSchKO –, GVBI S. 287). Nach Art. 32 BayDSG begutachtet der TÜV technische Fragen als Sachverständiger für die Aufsichtsbehörden über die Privatwirtschaft.

- Die Bekanntmachung des Bayer. Staatsministeriums des **Innern** vom 14. 7. 1978 zum **Vollzug des Bayer. Melderegengesetzes** (MABI S. 553), geändert durch Bekanntmachung vom 11. 9. 1978 (MABI S. 650), über die Auswirkungen des Datenschutzrechts auf das Melderecht – insbesondere die Erteilung von Auskünften aus dem Melderegister.
 - Die Bekanntmachung des Bayer. Staatsministeriums für **Unterricht und Kultus** vom 23. November 1978 mit erläuternden Hinweisen zum Vollzug der Datenschutzregisterverordnung (KMBI I 21/78, S. 585).
 - Die Bekanntmachung des Bayer. Staatsministeriums für **Unterricht und Kultus** vom 9. April 1979 mit erläuternden Hinweisen für die **Schulen** zum Vollzug des Bayerischen Datenschutzgesetzes (KMBI 9/79, S. 187).
 - Die Allgemeine Verwaltungsvorschrift des Bayer. Staatsministeriums für **Wirtschaft und Verkehr** für die Behandlung von Anzeigen nach den §§ 14 und 55 c der **Gewerbeordnung** vom 2. 1. 1980 (WVMBI S. 1). Dort wird unter Nr. 6 die Anwendung des Datenschutzgesetzes auf die Sammlung der Gewerbeanzeigen – besonders die Erteilung von Auskünften über Gewerbetreibende – geregelt.
 - Die Bekanntmachung des Bayer. Staatsministeriums für **Arbeit und Sozialordnung** zum Vollzug des § 139 b Abs. 1 Satz 3 der Gewerbeordnung (GewO) – Wahrung der Geheimhaltungspflicht bei **Gewerbeaufsichtsamtern** – vom 7. 11. 1980 (AMBI S. 262).
 - Die Bekanntmachung vom 29. 4. 1980 zum Vollzug datenschutzrechtlicher Vorschriften im Geschäftsbereich des Bayer. Staatsministeriums für **Ernährung, Landwirtschaft und Forsten** (LMBI 7/80, S. 51).
- Zum Vollzug des **BDSG** wird auf folgende Bestimmungen hingewiesen:
- Vollzugsbekanntmachung des Bayerischen Staatsministeriums des Innern vom 12. 7. 1978 (MABI S. 451), geändert durch Bekanntmachung vom 27. 3. 1981 (MABI S. 150), zu wichtigen **Anwendungsfragen**.
 - Vollzugsbekanntmachung des Bayerischen Staatsministeriums des Innern vom 30. 1. 1979 (MABI S. 22) über **Maßnahmen zur Datensicherung**.

1.2 Wesentlicher Inhalt der Datenschutzgesetze:

Hierzu finden sich im 1. und 2. Tätigkeitsbericht Ausführungen.

Anhang 2

Anschriften der Datenschutz-Kontrolle

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

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

Der Landesbeauftragte für den Datenschutz

Dr. Konrad Stollreither
Königinstr. 11, 8000 München 22, Tel. 0 89 / 2 37 03 - 3 41

2. Kontrolle des Datenschutzes bei Behörden des Bundes, wie z. B. Kreiswehersatzamt, Arbeitsamt, Post:

Der Bundesbeauftragte für den Datenschutz

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

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

Regional zuständige Aufsichtsbehörden:

Regierung von Oberbayern
Maximilianstr. 39
8000 München 22
(Tel. 0 89 / 21 76 - 2 30 oder 3 88)

Regierung von Niederbayern
Regierungsplatz 50
8300 Landshut
(Tel. 08 / 82 21)

Regierung der Oberpfalz
Emmeransplatz 8/9
8400 Regensburg
(Tel. 09 41 / 56 41)

Regierung von Oberfranken
Ludwigstr. 20
8580 Bayreuth
(Tel. 09 21 / 60 41)

Regierung von Mittelfranken
Schloß
8800 Ansbach
(Tel. 09 81 / 5 31)

Regierung von Unterfranken
Peterplatz 9
8700 Würzburg
(Tel. 09 31 / 38 01)

Regierung von Schwaben
Fronhof 10
8900 Augsburg
(Tel. 08 21 / 3 10 51)

Oberste Aufsichtsbehörde: Bayer. Staatsministerium des Innern
Odeonsplatz 3
8000 München 22
(Tel. 0 89 / 2 19 21)

Anhang 3

Stichwortverzeichnis

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

(römische Ziffer = Tätigkeitsbericht
arabische Ziffer = Seitennummer)

A	
Abgangskontrolle	III/30
Abiturientenbefragung	III/21, 22
Abschleppunternehmen	III/14
Absolventen	III/22
Adreßbücher	III/24
Adreßbuchverlage	I/11, II/18
Adreßdaten	I/11
Adrema-Platteien	II/27
ADV-Benutzer-Arbeitskreis	III/33
Änderungsgesetz zum Meldengesetz	II/10
Aktenvernichter	III/33
Aktenversand	III/17
Amt für Ausbildungsförderung	III/18
Anrufung Landesbeauftragten	III/5
Art. 15 BayDSG	II/8
Art. 26 BayDSG	II/9, III/8
Art. 8 Abs. 1 BayDSG	II/15
Aufbau Datenschutzregister	I/6, II/11
Aufbewahrung	II/27
Aufgaben des Landesbeauftragten	I/3
Auftragsdatenverarbeitung	II/26, III/8
Ausbildungsförderung	III/18
Auskunft	II/24, III/5
Auskunft Art. 8 Abs. 1 BayDSG	II/15
Auskunft Sicherheitsbereich	II/19
Auskunfteien	I/14
Auskunftssperre	I/12
Auskunftsverweigerung	III/29

B	
Banken	I/12, II/18
Basisdokumentation	II/21
Bauvorhaben	II/25
BayDSG	III/5
Bayer. Landeskriminalamt	III/15
Bayerischer Rundfunk	II/28, III/34
BDSG	III/5
Beamtenlaufbahn Versicherung	III/23
Behördenpersonal	III/24
Beirat	I/4, II/5, III/4
Beratung öffentliche Verwaltung	I/6, II/7
Beratung Staatsbürger	II/6
bereichsspezifische Regelung	III/5
Bereinigung der Sammlung	II/11
Berufsgenossenschaft	III/18
Berufsgruppen	I/11
Berufsverbände	II/23
Bestellung Datenschutzbeauftragter	III/18
Betriebssoftware-Systeme	III/9
Betriebszentrale	III/26
Betroffenen Begriff des	II/13
Bewerber Beamtenlaufbahn	III/23
Bezirk	III/18
Bibliotheken	I/16
Bildschirmtext	III/25
Breitbandkabelgesetz Rheinland-Pfalz	III/28
Breitbandkabelnetze	III/25

Bundeskindergeldgesetz	III/18	G	
Bundessozialhilfegesetz	III/18	Geburten	III/10
Bundesversorgungsgesetz	III/18	Geheimdienste	III/15
		Gemeinde	III/18
D		Gerichte	III/16
Dateibegriff	I/9, II/13	Geschäftsstelle	I/4
Daten	III/7, 12, 13	Geschäftsstellenpersonal	III/4
Datenübermittlung	I/8, II/18, 21, 23, III/13	Gesetzesvorhaben	II/8
Datenübermittlung Erforderlichkeit	II/14	gespeicherte Daten	III/5
Datenabgleich	III/14	gespeicherte Daten Sicherheitsbereich	II/19
Datenerhebung	I/5, II/7, 14, 22, III/21	Gesundheitsamt	III/18
Datengeheimnis	III/18, 19	Gesundheitsbereich	I/16, II/21, III/18
Datenlöschung	I/10	Gesundheitsbogen	III/20
Datensammlungen	II/10	Gesundheitskarten	III/20
Datenschutz Neue Medien	III/26	Gewerbekartei	II/24
Datenschutzbeauftragte	III/5	Glaubwürdigkeit kindlicher Zeugen	III/14
Datenschutzbeauftragte Interne	II/5, III/18	Gleitzeiterfassungskarten	III/24
Datenschutzkontrolle Neue Medien	III/26	Grenze	III/13
Datenschutzrecht	III/5	Großrechenzentrum	III/29
datenschutzrechtliche Freigabe	III/8	Grundeigentümer	I/12
Datenschutzregister	I/6, II/11, 12, III/4, 19	Grundsätze für die Verarbeitung	III/31
Datensicherung	I/5, II/8, 15	Grundstücksbewerber	II/26
Datensicherung Neue Medien	III/26	Gruppenauskünfte	I/13, II/18, III/10
Datensicherungsmaßnahmen	III/30, 31	GUIDE	III/34
Datenspeicherung Erforderlichkeit	II/14	Gutachtenverwaltung LKA	III/15
Datenträger	II/27		
Datenveröffentlichung	II/22	H	
Datenverarbeitung	I/5, 8, 16	Hauseigentümer	I/12
Datenverarbeitung Begriff	II/15	Hochschulbereich	II/22, III/20
Datenverarbeitung im Auftrag	III/8	Hochschule	III/19
Datenverarbeitungsprogramm	II/9, III/32	Hochschulinstitute	I/14, II/18
Datenweitergabe	II/22	Hochschulstatistikgesetz	III/22
dienstliche Telefongespräche	III/23		
Dienstprogramme	III/30	I	
Direkt-Werbung	III/10	Interne Datenschutzbeauftragte	II/5, III/18
		Intimsphäre	III/16
E		J	
ed-Bogen	III/13	Jubiläumsdaten	I/13, II/18
EDV-Organisation	II/26	Jugendamt	III/18
Effektivdaten	II/26	Jugendwohlfahrtsgesetz	III/18
Einsicht Sozialhilfeunterlagen	III/19	Justiz	III/16
Einsicht des DSB Verfassungsschutz	III/15		
Einsichtnahme Studentenkarteien	III/21	K	
Einwilligung	I/8	Kabelfernsehen	III/25
Einwilligung Speicherung Neue Medien	III/26	Kabeltext	III/25
Einwohnermeldewesen	I/10, II/17	Karteien	II/27
Entschädigung Strafverfolgungsmaßnahmen	III/17	Kernspeicherauszüge	II/26
Erfahrungsaustausch	I/7, II/13	Kfz-Zulassungsstellen	III/14
Erfassungskarten	III/24	Kfz-Zulassungsdaten	I/17
Erhebung des Namens	III/22	Kindergarten	III/21
Erhebung von Daten	III/7	Kindergeldabgleich	II/22
Ermächtigungsklausel	II/16	kindliche Zeugen Glaubwürdigkeit	III/14
Erweiterte Auskünfte	II/18	Kommunalbehörden	III/31
		Konferenz Datenschutzbeauftragte	III/5
F		Kontrolle	I/5
Fachhochschule	II/23, III/31	Kontrollzuständigkeit	III/7
Fernmeldegeheimnis	III/26	Kostenerhebung	I/9, II/15
Fernsehsatellit	III/25	KpS	II/11, III/12
Fernwartungsdienst	III/9	Krankenhäuser	III/20
Finanzamt	III/17	Kreditauskunfteien	III/29
Finanzverwaltung	II/23	Kreditinstitute	III/21
Formulare	I/5	Kreditschutzeinrichtungen	I/8
Forschung	II/26, III/19	Kriminalpolizeiliche Datensammlungen	II/10
freie Entfaltung der Persönlichkeit	III/16	Kriminalpolizeiliche Sammlung	III/12
Freigabe Art. 26 Abs. 2 und 4 BayDSG	I/6, II/9, III/8	KS-Richtlinien	III/13
		Kunsturhebergesetz	III/28

L

Landesbeauftragten Anrufung	III/5
Landesbeauftragter für den Datenschutz	I/4
Landesgesetz Breitbandkabel	III/28
Landesversicherungsanstalt	III/18
Landkreis	III/18
Landratsamt	III/31
Lebensgestaltung private	III/16
Lichtbilder	III/28
LKA	III/15
Löschung	I/10, II/14, III/13

M

Marktforschung	II/17
maschinenlesbarer Personalausweis	II/9, III/5
Maßnahmen nach Art. 15 BayDSG	III/29
Maßnahmenkatalog	II/16
Medien	III/25
Medienprivileg	III/26
Meinungsforschung	II/17
Meldeamt	I/13
Meldegesezt	II/10
Melderechts-Rahmengesetz	II/10, III/5
Melderegister	I/11-14, II/18-19, III/10
Meldescheine	III/10
Meldewesen	III/10
Meldung zum Datenschutzregister SGB X	III/19
Mikroprozessor-Technik	III/9
MiStra	II/22, III/16
Mitteilung Prüfungsergebnis	III/15
Mitteilung in Strafsachen	III/16
Mängel Datensicherung	II/8, III/29

N

Nebentätigkeiten	III/29
Neue Medien	III/9, 25
nichtöffentliche Stellen	II/25
Novellierung des BDSG	III/5
Nutzung Datenschutzregister	II/12
Nutzung von Daten	III/29
Nutzung von Statistikdaten	III/21

O

öffentlich-rechtliche Religionsgesellschaften	III/24
öffentliche Stellen	I/10
öffentliche Stellen Wettbewerbscharakter	II/15
öffentliche Verwaltung	I/6
Öffentliche Zustellung	III/28
Öffentliches Interesse	III/10
Öffentlichkeitsarbeit	I/6, II/12
Online-System	II/14
Ordnungsbegriff	II/26
Ordnungsmerkmale	I/14, II/9, III/5
Ortskrankenkasse	III/18

P

Papiervernichter	III/33
Parteien	I/13, II/18, III/10
Patientendaten	III/20
Persönlichkeitsentfaltung	III/16
Persönlichkeitsprofile	III/26
Personal der Geschäftsstelle	III/4
Personalausweis	II/9, III/5
Personaldaten	I/18, II/23
Personalnachrichten	III/24
Personalwesen	III/23

personenbezogene Daten	III/31
Personenkennzeichen	III/5
Planung	I/15, II/20, III/21
Planungsdatensammlungen	II/20, 21
Planungszwecke	III/22
Polizei	III/12, 13
private Lebensgestaltung	III/16
Prüfung Art. 15 BayDSG	
Rechenzentrum	II/8
Prüfungsergebnis Mitteilung	
Verfassungsschutz	III/15
Programmtest	II/26
Prozeßkostenhilfe	III/17
Psychiatrisch-Med. Basisdokumentation	II/21

R

Rasterfahndung	III/11
Rechenzentrum	II/8, 27
rechnergesteuertes Zugangskontrollsystem	III/33
Rechnerverbund	III/9
Rechtsfragen	I/8, II/13
Registrierung Gespräche	III/23
Registrierung Grenze	III/13
Reisende Registrierung	III/13
Religionsgesellschaften	III/24
Rückkanal	III/25
Rundfunk	II/28, III/34

S

Sanierungsmaßnahmen	II/21
Schülerausweise	III/21
Schülerbefragung	III/22
Schülerdaten	III/21
Schufa-Klausel	II/17
Schulbereich	I/17, II/22, III/20
Schuldnerverzeichnis	III/18
Schulen	II/22
Schutzstufen	II/16
Schutzwürdige Belange	I/9
SCOUT e. V.	III/33
Sekundarstufe II	III/22
SGB X	III/5, 18
Sicherheitsbereich	I/16, II/10, 19, III/11
Sonderschule	III/21
sonstige Verwaltungszwecke	III/21
Sozialhilfeunterlagen	III/19
Sozialamt	III/18
Sozialberatungsstelle	I/14
Sozialbereich	I/16, II/21, III/18
Sozialbericht	II/22
Sozialgeheimnis	III/5
Sozialgesetzbuch	III/5, 18
Sozialhilfeempfänger	III/22
Sozialhilfestatistik	III/22
Sozialhilfestelle	II/21
Sozialleistungsträger	III/18
Sparkassen	I/12, II/18
Speicherung Teilnehmerdaten	II/26
Sperrung	III/12
Staatsanwaltschaften	III/16, 17
Standardsoftware-Systeme	III/9
Standesamt	III/10
Statistik	I/15, II/20, III/21
Statistikdaten	III/21
Stellungnahme Gesetzesvorhaben	II/8
Steuerverwaltung	II/23, 24
Strafverfolgungsmaßnahmen	III/17
StrEG	III/17
Studentenkanzlei	III/31
Studentenkartei	III/21
Suchtkranke	II/22

T		Verwaltungsdaten	III/22
technische Zukunftsfragen	III/9	Verwaltungszustellungsgesetz	III/28
Teilnehmerdaten Neue Medien	III/26	Verwaltungszwecke	III/21
Telefongespräche	III/23	Videotext	III/25
Telekommunikationsbericht	III/25	W	
Temporäre Dateien	III/32	Weitergabe	II/26
Testbetrieb	III/30	Weitergabe Schülerdaten	III/21
U		Werbung	III/10
Übermittlung	II/25	Wettbewerbscharakter	II/15
Übermittlung Kfz-Zulassungsdaten	I/17	Wettbewerbscharakter öffentlichen Stellen	I/10
Übermittlung Melderegister	I/11-14	Wissenschaft	II/26
Übersicht Datenschutzregister	II/12, III/4	Wohngeldgesetz	III/18
Universitätskliniken	III/30	Wohnungsbauprämie	II/24
V		Z	
Verarbeitungsgrundsätze	III/31	Zentraldateien	III/17
Verfassungsschutz	III/15	Zeugen Glaubwürdigkeit kindlicher	III/14
Veröffentlichung	II/22	Zugangskontrolle	III/30
Veröffentlichung Standesamt	III/10	Zugangskontrollsystem	III/33
Verpflichtung	III/18	Zugriffskontrolle	III/30
Versendung von Akten	III/17	Zukunftsfragen technische	III/9
Versicherungen	I/8, III/23	Zulässigkeit Datenübermittlung	I/8
Versicherungswirtschaft	II/16	Zulässigkeit Datenverarbeitung	I/8
Vertrag Auftragsdatenverarbeitung	III/8	Zusammenarbeit	I/7, II/13