

8. Wahlperiode

30. 12. 80

Mitteilung

der Landesbeauftragten für den Datenschutz

**Erster Tätigkeitsbericht der Landesbeauftragten
für den Datenschutz**

Schreiben der Landesbeauftragten für den Datenschutz vom 29. Dezember 1980 Nr. C 2310:

Anbei übersende ich Ihnen meinen ersten Tätigkeitsbericht, den ich nach § 16 Abs. 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 31. Dezember 1980 zu erstatten habe.

Dr. Ruth Leuze

**Erster Tätigkeitsbericht
der
Landesbeauftragten für den Datenschutz
in Baden-Württemberg**

INHALTSVERZEICHNIS

	Seite
1. Teil: Zur Situation des Datenschutzes	7
1. Was heißt Datenschutz?	7
2. Hemmnisse bei der Verwirklichung des Datenschutzes	8
3. Aufbau des neuen Amtes	9
3.1 Erwartungshorizont	9
3.2 Aufbau der Dienststelle	9
3.3 Aufgabenbereich	9
3.3.1 Sachliche Zuständigkeit	9
3.3.2 Örtliche Zuständigkeit	10
3.4 Reaktionen auf das neue Amt	10
3.4.1 Reaktionen aus dem Bereich der Politik	10
3.4.2 Reaktion der Verwaltung	10
2. Teil: Wahrnehmung der einzelnen gesetzlichen Aufgaben	11
1. Anwalt der Bürger	11
1.1 Reaktion der Bevölkerung	11
1.2 Anliegen der Bürger	11
1.3 Zur Aufsplitterung der Datenschutzkontrolle	12
1.4 Zur Notwendigkeit der Stärkung des Datenschutzbewußtseins	13
2. Kontrolltätigkeit	13
2.1 Allgemeines	13
2.1.1 Zur Kontroverse wegen der Kompetenzen	14
2.1.2 Arbeitsweise im Rahmen der Kontrolltätigkeit	14
2.2 Einzelne Kontroll- und Informationsbesuche	15
2.3 Konsequenzen	15
3. Beratungstätigkeit	15
3.1 Allgemeines	15
3.2 Einzelne Beratungen	16
3.3 Mitwirkung an der Gesetzgebung	16
3.4 Expertenkommission „Neue Medien“	16
4. Datenschutzregister	16
4.1 Sinn und Zweck	16
4.2 Datenschutzregisterverordnung	17
4.3 Aufbau des Datenschutzregisters	17
5. Öffentlichkeitsarbeit	18
5.1 Informationsblatt „Datenschutz – Chance und Aufgabe“	18
5.2 Veröffentlichungen und Vorträge	18
5.3 Fortbildung	18

	Seite
3. Teil: Schwerpunkte der bisherigen Tätigkeit	18
1. Abschnitt: Öffentliche Sicherheit und Ordnung	18
1. Polizei	18
1.1 Polizeiliche Informations- und Auskunftssysteme	18
1.1.1 INPOL-Neuordnung	18
1.1.2 Personenauskunftsdatei des Landes (PAD)	20
1.1.3 KpS-Richtlinien	22
1.1.4 Dateien-Richtlinien	23
1.1.5 Vereinfachtes Verfahren zur Bearbeitung von Bagatelldelikten	24
1.2 Probleme der polizeilichen Praxis in Baden-Württemberg	25
1.2.1 INPOL-Abfrage bei Zeugen und Anzeigerstattem	25
1.2.2 Auskunftserteilung an Bürger	26
1.2.3 Tagesberichte der Polizei	27
2. Verfassungsschutz	27
3. Staatsanwaltschaften und Strafgerichtsbarkelt	28
3.1 Anordnung über Mitteilungen in Strafsachen	28
3.2 Zentrale Namenskartei bei den Staatsanwaltschaften	29
4. Verkehrswesen	30
4.1 Erhebung personenbezogener Daten im Bußgeldverfahren	30
4.2 Bußgeldkarteien	31
4.3 Führerscheinkarteien	31
4.4 Karteien über eingestellte Strafverfahren nach § 153 a StPO	32
5. Meldewesen	33
5.1 Allgemeines	33
5.2 Handhabung des geltenden Melderechts	34
5.2.1 Erhebung von Meldedaten	34
5.2.2 Speicherung von Meldedaten	34
5.2.3 Übermittlung von Meldedaten	34
5.2.4 Erteilung von Auskünften an Einwohner	40
5.2.5 Sperrung und Löschung von Meldedaten	40
5.2.6 Datensicherungsmaßnahmen	40
5.3 Melderechtsrahmengesetz und künftiges Landesmeldegesetz	40
5.3.1 Melderechtsrahmengesetz	40
5.3.2 Landesmeldegesetz	41
6. Paßwesen	42

	Seite
2. Abschnitt: Gesundheits- und Sozialwesen	43
1. Gesundheitswesen	43
1.1 Gesundheitsämter	43
1.1.1 Vordrucke	43
1.1.2 Aufbewahrung von Karteikarten und Akten	44
1.1.3 Dateien	44
1.1.4 Schulgesundheitspflege	44
1.1.5 Sammlung der Durchschriften ausgestellter Bescheinigungen über die soziale Beratung Schwangerer nach § 218 b Abs. 1 Satz 1 StGB	45
1.1.6 Sammlung der Leichenschauscheine	46
1.2 Krankenhäuser	48
1.3 Krebsregister	48
1.4 Versand von ärztlichen Anamnesebogen	49
2. Sozialwesen	50
2.1 Auswirkung der Neuregelungen des Sozial- geheimnisses	50
2.2 Datenerhebung bei Gewährung von Zuwendungen	51
2.3 Sozialhilfestatistik	52
3. Abschnitt: Schulen und Hochschulen	52
1. Schulen	52
1.1 Übermittlung von Schülerdaten	52
1.2 Schulvergleich	53
2. Hochschulen	54
4. Abschnitt: Steuerverwaltung	55
1. Anwendung des Landesdatenschutzgesetzes in der Steuerverwaltung	55
1.1 Auskünfte an Bürger	55
1.2 Steuergeheimnis	56
1.3 Verwendung von Adreßaufklebern	56
5. Abschnitt: Allgemeine Verwaltung	57
1. Personalwesen	57
1.1 Führung von Personalkarteien	57
1.2 Automatisierte Verfahren zur Unterstützung der Personalverwaltung	57
1.3 Registrierung dienstlicher und privater Telefongespräche	58
2. Kommunale Angelegenheiten	59
2.1 Nutzung von Unterschriftenlisten für Bürger- begehren zu anderen Zwecken	59
2.2 Vergabe von Grundstücken	59
2.3 Akten über Einwohner	60
3. Aktenaussonderung und Archivverwaltung	60
4. Statistik	61

	Seite
6. Abschnitt: Datenverarbeitung	61
1. Stand der Datenverarbeitung	61
2. Weiterentwicklung der automatisierten Datenverarbeitung	62
3. Datensicherung	62
3.1 Datensicherung in der manuellen Datenverarbeitung	62
3.2 Datensicherung in der automatisierten Datenverarbeitung	63
4. Teil: Neue Medien	65
1. Datenschutzprobleme der neuen Medien	65
2. Zielvorstellungen	65
3. Möglichkeiten zur Realisierung der Zielvorstellungen	67
5. Teil: Erfahrungen mit dem Landesdatenschutzgesetz	68
1. Anwendungsbereich des Landesdatenschutzgesetzes	68
1.1 Datei	68
1.2 Interne Datei	69
1.3 Beschränkung auf Datenverarbeitung ohne Datenerhebung	70
2. Datengeheimnis	70
3. Hinweispflicht	71
4. Datenübermittlung	72
5. Datenverarbeitung im Auftrag	73
6. Sperrung und Löschung	74
7. Verwaltungsvorschriften	75
8. Wissenschaftliche Forschung	75
6. Teil: Fortentwicklung des Datenschutzrechts	76
1. Novellierung des Bundesdatenschutzgesetzes	76
2. Bereichsspezifische Regelungen	77
2.1 Bedürfnis	77
2.2 Gefahren	77
2.3 Forderung	78
Schlußbemerkung	78

1. Teil: Zur Situation des Datenschutzes

1. Was heißt Datenschutz?

Das Schlagwort „Datenschutz“ ist in vieler Munde. Doch nur wenige verbinden eine klare Vorstellung mit ihm. Ziel des Datenschutzes ist, in unserer hochentwickelten Informationsgesellschaft den Mißbrauch persönlicher Daten zu verhindern. Datenschutz ist also nichts anderes als einer der wichtigsten Garanten unseres Grundrechts auf freie Entfaltung der Persönlichkeit. Er sichert unsere Privatsphäre, indem er jedem Übereifer wehrt, über uns möglichst viele Daten zu erheben, zu sammeln und zu verwerten. Datenschutz steckt die durch die Technik weit vorgerückten Grenzen zu einer totalen Information im Persönlichkeitsbereich neu ab. Seine Aufgabe ist, den angemessenen Ausgleich zwischen Informationsbedürfnis und Informationszwang einerseits und der Wahrung des Personseins andererseits in Staat und Gesellschaft, am Arbeitsplatz und im privaten Lebenskreis zu sichern. Außerdem will er den Umgang mit unseren persönlichen Daten transparent machen. Wie wichtig dies ist, zeigt allein der Umstand, daß nicht einmal ich weiß, wer welche meiner persönlichen Daten seit wann, wie lange und zu welchem Zweck sammelt und wie oft er sie an andere Stellen weitergibt. Solche Unkenntnis ist nicht gut; sie beunruhigt und verunsichert. Zudem hält sie den Bürger in Unmündigkeit anstatt ihn, wie es Ziel des demokratischen Rechtsstaats sein muß, frei entscheiden zu lassen, was er aus seiner Privatsphäre preisgibt.

Datenschutz ist keine Modeerscheinung. Gewiß, die Terminologie ist neu. Seine Zielsetzung aber ist unserer Rechtsordnung — wenn auch nicht in voller Breite — seit langem vertraut. Zu ihrer Tradition gehören eine Vielzahl datenschutzrechtlicher Regelungen. Ich denke zum Beispiel an das Arzt-, Steuer-, Bank- und Postgeheimnis, die Verwertungsverbote im Strafrecht und Zeugnisverweigerungsrechte. Die Datenschutzgesetze vervollständigen diesen bunten Strauß von Datenbestimmungen mit dem Ziel, die offensichtlichen Lücken unseres Rechts in dem besonders wichtigen Bereich der Datenverarbeitung in Dateien zu schließen. Datenschutz beschränkt sich aber keineswegs hierauf; er erfaßt alle Verwaltungsvorgänge, die den Umgang mit unseren Daten betreffen. Die Handhabung in der Sache ist entscheidend, nicht die Form, in der sie geschieht.

In dieser Sicht bestärkt mich die Bevölkerung. Der Bürger will wissen, ob die Verwaltung seine persönlichen Daten erfragen, sammeln, weitergeben oder sonstwie verwerten darf. Hierzu erwartet er mit Recht eine klare Antwort. Ihn interessiert dagegen überhaupt nicht, welches Hilfsmittel die Verwaltung sich hierbei bedient. Ihm ist gleichgültig, ob die Verwaltung seine Daten in Karteien, Akten, Listen, Lose-Blatt-Sammlungen oder Formularen führt. Und schlichtes Unverständnis würde bei ihm auslösen, wenn er hören müßte, daß die Antwort auf seine Frage je nach Art des verwandten Hilfsmittels unterschiedlich ausfällt.

Mein Verständnis vom Datenschutz teilen auch die meisten Bereiche der Verwaltung des Landes Baden-Württemberg. Nur ganz vereinzelt stellt sie meine Sicht in Frage und ist bestrebt, mich auf die behördliche Datenverarbeitung in Dateien zurückzudrängen. Dieser Versuch stimmt so bedenklich, weil er darauf abzielt, nicht nur mein Betätigungsfeld entgegen dem klaren Gesetzauftrag empfindlich einzuengen sondern zugleich — und das ist das letztlich Entscheidende — die Rechtsposition des Bürgers erheblich zu verkürzen. Was hätte meine Datenschutzkontrolle eigentlich noch für einen Sinn, wenn es mir als Anwalt der Bürger verwehrt wäre,

z. B. die Beachtung des Wahlgeheimnisses, die Bepunktung und Verwertung eingestellter Strafverfahren, die Datenübermittlung aus Personalakten, die Vernichtung von Polizeiakten über unschuldig angezeigte Bürger zu überprüfen? Ich bin fest entschlossen, mein Amt als Sachverwalter des Datenschutzes ohne jede Einschränkung auszuüben.

2. Hemmnisse bei der Verwirklichung des Datenschutzes

Die Verwirklichung des Datenschutzes in der öffentlichen Verwaltung ist nicht einfach. Dies hat verschiedene Gründe:

- Die Datenverarbeitung befindet sich im Umbruch in eine ungewisse Zukunft, das Recht des Datenschutzes steckt trotz erheblicher Aktivitäten der letzten Jahre in den ersten Anfängen. Kaum jemand wird deshalb wagen, den Standort von Datenverarbeitung und Datenschutz exakt zu bestimmen und zuverlässige Prognosen abzugeben. Sicher werden die Entwicklungen im technischen und rechtlichen Bereich voranschreiten. Dies wird umso eher der Fall sein, je früher unser heutiges noch weitgehend geschlossenes System der Datenverarbeitung zunehmend durch ein offenes, von allen Seiten zugängliches System ersetzt wird. Der Austausch persönlicher Informationen wird damit leichter und häufiger, das Bedürfnis nach Information verstärkt, die Informationsnutzung gesteigert. Wie sich der Schutz der Persönlichkeitssphäre bei solchen Veränderungen am besten gewährleisten läßt, ist offen. Nichts scheint mir daher wichtiger, als die sich anbahnende Entwicklung aufmerksam zu begleiten und immer wieder die Frage nach der angemessenen datenschutzrechtlichen Aktion und Reaktion zu stellen.
- Trotz viel guten Willens und redlichen Mühens herrscht bei einer Vielzahl öffentlicher Stellen große Unsicherheit über die Bedeutung des Datenschutzes. Das nimmt nicht weiter wunder, weil das Datenschutzrecht ein junges und dazu sehr schwieriges Rechtsgebiet ist. Die Abstraktion seiner Sprache und das Fehlen einer allgemein verständlichen Information der Behörden über die Bedeutung des Datenschutzes tragen weiter dazu bei. Eine meiner wichtigsten Aufgaben ist daher, die Kenntnisse der Behörden im Datenschutzrecht zu vertiefen und ihr Verständnis für den Datenschutz zu stärken.
- Auch haben sich in der öffentlichen Verwaltung Untugenden eingeschlichen, die der Durchsetzung des Datenschutzes entgegenstehen. Ich denke hierbei an die weit verbreitete Neigung,
 - die abgewogene Einzelentscheidung zunehmend durch schematisierte Bescheide zu ersetzen
 - aus Neugier mehr Daten als die unbedingt benötigten zu erheben
 - persönliche Daten aus Bequemlichkeit nicht direkt beim Bürger, sondern bei anderen öffentlichen Stellen zu erfragen und dadurch den Bürger zum Objekt staatlicher Informationspolitik zu machen
 - fehlende Orientierung durch viele Informationen zu ersetzen
 - Informationen zur Entlastung von eigener Verantwortung wahllos zu streuen
 - Datenschutz als Vorwand für mangelnde Bereitschaft zum Verwaltungshandeln oder als Begründung nicht plausibler Verwaltungsentscheidungen zu benutzen.

3. Aufbau des neuen Amtes

3.1 Erwartungshorizont

Mit meinem Amt verknüpfen sich die unterschiedlichsten Erwartungen. Die Bürger setzen auf mich als Verfechter ihrer Interessen, die Verwaltung möchte einen milden Kontrolleur, die Öffentlichkeit gelegentlich griffige und sensationelle Nachrichten. Wichtig im Widerstreit dieser Wünsche ist, sich nicht in die eine oder andere Richtung drängen zu lassen. Mein Amt kann auf Dauer nur stark sein, wenn es stets fachlich qualifiziert arbeitet, offen und ehrlich gegenüber Bürgern wie Verwaltung für seine Ziele eintritt und unabhängig von Lob oder Tadel konstant und beharrlich seine Aufgaben wahrnimmt. Spektakuläre Erfolge lassen sich auf diese Weise nicht erzielen, wohl aber — so hoffe ich zumindest — Vertrauen und Glaubwürdigkeit. Gerade dies ist aber unerlässlich, will man dem Datenschutz in der richtigen Weise zum Durchbruch verhelfen.

3.2 Aufbau der Dienststelle

Die einmütige Haltung von Landesregierung und Landtag, mich zur Landesbeauftragten für den Datenschutz zu bestellen, war die beste Starthilfe für das neue Amt. Dieses trat ich am 1. April 1980 wenige Tage nach Inkrafttreten des Landesdatenschutzgesetzes an. In den ersten Wochen ging es darum, neben der Vielfalt der einstürmenden Anfragen und fachlichen Probleme die organisatorischen Voraussetzungen für einen wirksamen Dienstbetrieb zu schaffen.

- Dank der nachhaltigen Unterstützung des Innenministeriums waren bereits im Laufe des April alle im Nachtragshaushalt 1980 für meine Dienststelle ausgewiesenen Stellen besetzt. Zwei Juristen, ein EDV-Praktiker, zwei Verwaltungsbeamte und drei Verwaltungsangestellte sind meine acht Mitarbeiter. Sie haben durch ihre gediegenen Kenntnisse, ihre stete Einsatzbereitschaft, ihr Engagement und ihre geschickte Art im Umgang mit Behörden und Bürgern wesentlich zum raschen Aufbau und Ansehen meines Amtes beigetragen. Dafür danke ich allen sehr herzlich.
- Durch die tatkräftige Mithilfe der Staatl. Liegenschaftsverwaltung fand ich nach einer provisorischen Unterkunft im Innenministerium geeignete Diensträume. Für die Ausstattung bewilligten mir Innen- und Finanzministerium die notwendigen überplanmäßigen Mittel.

Auf diese Weise gelang es, in nur kurzer Zeit den organisatorischen Aufbau der Dienststelle abzuschließen.

3.3 Aufgabenbereich

3.3.1 Sachliche Zuständigkeit

Das Landesdatenschutzgesetz weist mir vor allem die Aufgaben zu,

- als Anwalt der Bürger sich deren Fragen zum Datenschutz anzunehmen
- die Verwaltung des Landes Baden-Württemberg in Angelegenheiten des Datenschutzes zu kontrollieren und zu beraten
- auf Wunsch für Landtag und Landesregierung Gutachten zu aktuellen Fragen des Datenschutzes zu erstatten
- ein Datenschutzregister zu führen.

3.3.2 Örtliche Zuständigkeit

Meiner Datenschutzkontrolle und -beratung unterliegt die gesamte Verwaltung des Landes Baden-Württemberg. Niemand weiß genau, wie viele Stellen hierzu gehören; denn es gibt kein amtliches Verzeichnis. Zählt man Gemeinden, Landkreise, Zweckverbände und sonstige kommunale Körperschaften, die staatlichen Behörden des Landes, Schulen, Hochschulen und sonstige Organisationen des öffentlichen Rechts zusammen, müßten es rund 10 000 Stellen sein. Ich bin mir der Schwierigkeiten wohl bewußt, bei der geringen Größe meiner Dienststelle diesem umfangreichen Aufgabengebiet gerecht zu werden. Stets werde ich Schwerpunkte setzen müssen und nur ausgewählte Behörden beraten und kontrollieren können. Diese Tätigkeit hat aber Pilotfunktion; sie läßt allgemeine Schlüsse zu und wirkt sich damit auf das Verwaltungshandeln der anderen Behörden aus.

3.4 Reaktionen auf das neue Amt

3.4.1 Reaktionen aus dem Bereich der Politik

Im politischen Raum fand ich großes Verständnis für meine Tätigkeit.

- Der neugewählte Landtag von Baden-Württemberg regelte dankenswerterweise in seiner Geschäftsordnung meine Rechtsstellung im Verhältnis zum Parlament. Insbesondere räumte er mir im Rahmen meiner Aufgaben Zutritt zu und Rederecht in den Ausschusssitzungen ein.
- Die Landesregierung ließ mir jede Freiheit in Aufbau und Führen meines Amtes. Ihre Aufgeschlossenheit in Fragen des Datenschutzes ist für mich hilfreich.
- Auch der Herr Innenminister, der die Dienstaufsicht über mich hat, achtete nicht nur stets meine Unabhängigkeit, sondern unterstützte mich bei meinen Anliegen.

Die Zuordnung meines Amtes zum Innenministerium, die für mich keine Grundsatzfrage ist, brachte keine Nachteile. An dieser Bewertung änderte auch nichts die Diskussion über meine Kompetenzen, welche das Innenministerium gleich zu Beginn meiner Tätigkeit nicht nur im Lande gegenüber den anderen Ressorts und kommunalen Landesverbänden, sondern auch auf Bundesebene eröffnete. Diese Aktion hätte es bei einer anderen Zuordnung meines Amtes ebenfalls gegeben. Denn die Ursache ist nicht der Wunsch nach politischer Einflußnahme auf meine Amtsführung, sondern das Bestreben eines Zweiges der Innenverwaltung, sich zum Koordinator und Sprecher des Datenschutzes zu machen, und die Befürchtung, das neu geschaffene externe Kontrollorgan könnte zu große Einwirkungsmöglichkeiten auf die Verwaltung erhalten. Ich bedaure, daß gerade die Stelle der Landesverwaltung, die kraft ihres Auftrags meine Arbeit am meisten unterstützen müßte, dies am wenigsten tut.

3.4.2 Reaktion der Verwaltung

Im übrigen zeigte sich die Verwaltung gegenüber dem neuen Amt aufgeschlossen. Mehr kann der Kontrolleur vom Kontrollierten nicht erwarten.

- Zu den Gemeinden, Städten, Landkreisen und ihren Landesverbänden ergaben sich rasch gute Kontakte. Die Zusammenarbeit ist sehr erfreulich.
- Auch alle Landesbehörden der mittleren und unteren Ebene akzeptieren das neue Amt und wenden sich mit zunehmendem Vertrauen hierher. Mehrfach erlebte ich sogar bereits, daß Behörden um meine Kontrolle baten.
- Ebenso bestehen zu den Ministerien gute Kontakte. Die anfangs starke Zurückhaltung der Datenschutzstellen einiger Ressorts ist weitgehend überwunden. Grund hierfür war nicht nur die anfängliche Unkenntnis über die Arbeitsweise des neuen Kontrollorgans, sondern auch die Unsicherheit dieser Stellen in Fragen des Datenschutzes und vor allem ihre Unkenntnis, wie es die nachgeordneten Behörden mit dem Datenschutz halten.

2. Teil: Wahrnehmung der einzelnen gesetzlichen Aufgaben

1. Anwalt der Bürger

1.1 Reaktion der Bevölkerung

Die Bürger Baden-Württembergs haben in ihrer Mehrzahl die Verabschiedung des Landesdatenschutzgesetzes weder erwartet noch gefordert. Ihr Interesse wurde erst geweckt, als sie dieses Gesetz in ihr Leben einbeziehen und daran Hoffnungen und Erwartungen knüpfen konnten. Dann allerdings entfalteten viele eine für mich geradezu erstaunliche Aktivität. Seit meiner Ernennung zur Landesbeauftragten für den Datenschutz wenden sich täglich Bürger mit ihren Sorgen an mich, die sie wegen des Umgangs der öffentlichen Verwaltung mit ihren persönlichen Daten bedrücken. Meine vornehmste Aufgabe ist, sich dieser Anliegen anzunehmen. Alle Informationen der Bürger behandle ich vertraulich. Den Behörden teile ich nur die zur Aufklärung des Sachverhalts nötigen Umstände mit. Oft vergehen Wochen, wenn nicht sogar Monate, bis ich dem Bürger mein Prüfergebnis mitteilen kann. Dies bedaure ich sehr. Ich fürchte freilich, hieran wird sich in Zukunft nichts Entscheidendes ändern, da die notwendigen Recherchen und Verhandlungen mit den Behörden im Regelfall viel Zeit beanspruchen. Umso erleichterter bin ich über die Geduld der Bürger; sie nehmen Wartezeiten hin, wenn sie nur wissen, daß man ihren Anliegen nachgeht.

Andererseits schrecken die Bürger meist zurück, bei den Behörden selbst ihr Recht auf Auskunft über die gespeicherten Daten geltend zu machen. Ich wage keine abschließende Erklärung dieses Phänomens. Eine Rolle spielen dürfte das Gefühl, wegen der Kompliziertheit des Rechts und der fehlenden Transparenz des Verwaltungshandelns als einzelner ohne fachliche Vorbildung der Verwaltung unterlegen zu sein. Ich habe den Eindruck, daß die Durchsetzung der Bürgerrechte im Datenschutz heute noch vielfach eine Bildungsfrage ist. Deshalb liegt mir besonders daran, gerade den einfachen Menschen ohne besondere Vorbildung zu erreichen und ihm bei der Durchsetzung seiner Datenschutzbelange zu helfen.

1.2 Anliegen der Bürger

Die Bürger wenden sich mit den verschiedensten Anliegen an mich. Durch manche Hinweise wurde ich auf Grundsatzprobleme

des Datenschutzes in der Verwaltung aufmerksam. Aus der Fülle der Bürgeranliegen will ich nur einige Beispiele nennen:

- Auffallend stark ist das Interesse an allgemeinen Fragen des Datenschutzes und die Nachfrage nach Informationsmaterial.
- Viele Bürger wollen wissen, welche Behörden über sie welche Daten speichern. Manche interessieren sich besonders für eine etwaige Datenspeicherung bei der Polizei.
- Andere beklagen, ihre Daten seien zu Unrecht gespeichert. Ich denke z. B. an einen Mann, der stets pünktlich seine Grundsteuer bezahlte, trotzdem aber durch ein Versehen der Stadtverwaltung im Rechenzentrum als säumiger Steuerzahler geführt wurde.
- Viele Eingaben betreffen die Erhebung persönlicher Daten für statistische Zwecke, z. B. für den Mikrozensus, die Hochschulstatistik oder das Erstellen eines Mietspiegels.
- Oft geht es bei den Eingaben um die Herausgabe von Adreß- und Ortssippenbüchern, die Veröffentlichung von Jubiläumsdaten, die Bekanntgabe von Namen und Anschriften einzelner Bevölkerungsgruppen, z. B. von Senioren und Jungwählern, an die Parteien für Zwecke der Wahlwerbung.
- Nicht selten sind Bürger verärgert, weil ihnen nach Erwerb eines Kraftfahrzeugs Werbematerial ins Haus geschickt wird.
- Nach Meinung vieler Bürger verlangen die Behörden mehr Angaben als sie zur Bearbeitung ihrer Gesuche benötigen, z. B. bei der Berechnung von Anwärterbezügen, der Bewilligung von Ausbildungsförderung oder der Aufnahme in Krankenanstalten.
- Unmut äußern die Bürger über die Unterrichtung einer Vielzahl von Stellen, insbesondere der Polizei, bei der Aufnahme eines Gewerbebetriebs.
- Viele befürchten eine unzulässige Ausforschung der Privatsphäre. Ich denke z. B. an einen übereifrigen Steuerfahnder, der von einem inserierenden Heiratsinstitut den Namen einer ehewilligen „jüngeren vermögenden Unternehmerin“ wissen wollte.
- Unmut lösen auch häufig Auskünfte aus dem Schuldnerverzeichnis aus.

1.3 Zur Aufsplitterung der Datenschutzkontrolle

In der Öffentlichkeit ist weitgehend unbekannt, daß die Datenschutzkontrolle im Lande — z. B. anders als in den Ländern Bremen, Saarland und Schleswig-Holstein — zwischen öffentlichem und privatem Bereich aufgeteilt ist. Mir obliegt die Kontrolle der öffentlichen Verwaltung; die Kontrolle der Datenverarbeitung durch private Personen oder Stellen hat die Landesregierung dagegen durch Verordnung von 1977 dem Innenministerium als Aufsichtsbehörde übertragen. Mich erreichen viele Anliegen von Bürgern, die den privaten Bereich betreffen. Dabei geht es z. B. um das Verhalten von Kreditschutzorganisationen, Heiratsinstituten, Adreßverlagen, Großversandhäusern, Datenübermittlungen im Rahmen von Bewerbungen oder bestehenden Arbeitsverhältnissen, Zusendung von Werbematerial. Die Enttäuschung der Bürger ist groß, wenn ich sie infolge der bestehenden Zuständigkeitsregelung an das Innenministerium als Aufsichtsbehörde verweisen muß. Viele äußern auch Unmut und Ärger, eine Datenschutzbeauftragte zu haben, die nun gerade in ihrem Fall nicht tätig werden kann. Für diese Reaktion habe ich großes Verständnis. Die Bürger sind mit der Unterscheidung von

Datenschutz im öffentlichen und im privaten Bereich und der daran geknüpften getrennten Kontrollzuständigkeit überfordert. Dies gilt umso mehr, als sich selbst Kenner des Datenschutzes oft schwer tun, bestimmte Vorgänge dem öffentlichen oder dem privaten Bereich zuzuordnen. Besonders schlecht sind die Bürger dran, deren Anliegen teils den öffentlichen, teils den privaten Bereich betreffen. Sie laufen Gefahr, widersprechende Auskünfte zu erhalten.

Die gegebene Zuständigkeitssplitterung der Kontrolle im Datenschutz ist daher alles andere als bürgerfreundlich. Auch hindert sie eine einheitliche Handhabung der Datenschutzkontrolle im öffentlichen und privaten Bereich, soweit es um die Anwendung gleichartigen Rechts geht. Schließlich führt sie zu einer Fülle von Doppelarbeit und widerstreitet dem Bemühen um Rationalisierung und Personaleinsparung in der öffentlichen Verwaltung. Trotz aller Verfestigungen, die die Trennung zwischen Kontrolle im öffentlichen und privaten Bereich schon erfahren hat, wäre es deshalb gut, ihre Vor- und Nachteile nochmals leidenschaftslos zu bedenken und im Interesse des Bürgers auch andere Lösungen zu erwägen.

1.4 Zur Notwendigkeit der Stärkung des Datenschutzbewußtseins

Die zahlreichen Aktivitäten der Bürger dürfen nicht darüber hinwegtäuschen, daß ihr Verständnis von Datenschutz keineswegs Allgemeingut ist. Ein nicht geringer Teil unserer Mitbürger steht heute noch den Problemen des Informationswesens und Datenschutzes gleichgültig gegenüber und glaubt, nicht betroffen zu sein. Ein kleiner Teil unserer Bevölkerung ist sogar mißtrauisch oder bereits dem Vorurteil verfallen, Datenschutz sei unnötiger Luxus und verhindere vernünftiges Verwaltungshandeln. Sehr vereinzelt erreichen mich Bürgerschriften dieses Inhalts. In diesen Fällen suche ich besonders das Gespräch und bemühe mich, die Aspekte des Datenschutzes verständlich zu machen. Im übrigen halte ich es für unerlässlich, jede Gelegenheit zu nutzen, das Datenschutzbewußtsein unserer Bevölkerung zu stärken.

2. Kontrolltätigkeit

2.1 Allgemeines

Die besten Regelungen nützen wenig, wenn sie nicht auch tatsächlich eingehalten werden. Dazu bedarf es einer wirksamen Kontrolle. Ganz besonders gilt dies für den Bereich des Datenschutzes, weil sich hier sehr viele Vorgänge behördenintern abspielen und der Betroffene nur selten davon erfährt. Der Gesetzgeber entschied sich deshalb aus guten Gründen dafür, diese Kontrolle einem unabhängigen, nicht in die Verwaltungshierarchie eingegliederten Organ zu übertragen. Zu diesem Zweck schuf er das Amt des Landesbeauftragten für den Datenschutz. Seine Kontrollaufgabe ist in § 16 Abs. 1 Satz 1 LDSG näher umschrieben. Danach hat er die Einhaltung der Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen zu überwachen. Meine Aufgabe ist daher, nicht nur auf die Einhaltung des Landesdatenschutzgesetzes zu achten, sondern auch die Beachtung aller anderen Vorschriften über den Datenschutz sicherzustellen. Diese Aufgabenzuweisung trägt dem Umstand Rechnung, daß das Landesdatenschutzgesetz den Datenschutz nicht umfassend und abschließend regelt, sondern daß es daneben noch eine große Zahl anderer Vorschriften mit datenschutzrechtlicher Zielsetzung gibt, wie z. B. die Regelungen über Berufsgeheimnisse, das Sozialgeheimnis und das Steuergeheimnis.

2.1.1 Zur Kontroverse wegen der Kompetenzen

Im Gegensatz zu meiner Sicht vertritt das Innenministerium die Auffassung, der Landesbeauftragte für den Datenschutz könne die Einhaltung der Vorschriften über den Datenschutz nur dann kontrollieren, wenn eine Verarbeitung von in Dateien gespeicherten Daten stattfindet. Ich kann diese Auffassung nicht teilen, weil sie

- dem klaren Wortlaut des § 16 Abs. 1 LDSG widerspricht,
- dem Bemühen des Landtags, während der intensiven Beratungen des Landesdatenschutzgesetzes die Stellung des Landesbeauftragten zu stärken, nicht Rechnung trägt,
- den engen Zusammenhang zwischen Kontroll- und Beratungstätigkeit außer acht läßt,
- die Möglichkeiten des Landesbeauftragten für den Datenschutz, Anwalt der Bürger zu sein, in unvertretbarem Maße einschränken würde.

Vor allem aber würde sie auch zu völlig willkürlichen und unverständlichen Ergebnissen führen. Wäre ich, wie dem Innenministerium vorschwebt, auf die Kontrolle von Datenverarbeitungsmaßnahmen mit Dateibezug beschränkt, würden oft organisatorische Zufälligkeiten über meine Kontrollbefugnis entscheiden. Ein kleines Beispiel mag dies verdeutlichen. Solange das Grundbuch in Lose-Blatt-Form geführt wird, könnte ich überprüfen, ob unter Verletzung von § 12 der Grundbuchordnung Einsicht in das Grundbuch gewährt wurde, da bei dieser Art der Grundbuchführung die Sammlung der verschiedenen Grundbuchblätter eine Datei ist. Sobald diese Blätter aber gebunden sind, würde meine Prüfungskompetenz entfallen, da ein Buch keine Datei im Sinne des Landesdatenschutzgesetzes darstellt. Ein solch sinnwidriges Ergebnis wollte der Gesetzgeber aber nicht. Ich legte meine, auch vom Justizministerium geteilte Auffassung, von der ich bei meinen Kontrollmaßnahmen ausgehe, den Ministerien und den kommunalen Landesverbänden im einzelnen dar und gehe davon aus, daß sie die meiner Kontrolle unterliegenden Behörden respektieren.

2.1.2 Arbeitsweise im Rahmen der Kontrolltätigkeit

Im Rahmen meiner Kontrolltätigkeit erwies es sich neben dem Einholen schriftlicher Stellungnahmen vor allem als zweckmäßig, Kontroll- oder Informationsbesuche durchzuführen. Ziel der Kontrollbesuche ist, das konkrete Vorgehen einer einzelnen Stelle in datenschutzrechtlicher Hinsicht zu überprüfen. Dabei umfaßt die Kontrolle entweder die gesamte Tätigkeit oder erstreckt sich nur auf einzelne Aufgabengebiete der Behörde. Informationsbesuche dienen vor allem dazu, mir einen Überblick über die Tätigkeit der Behörde zu verschaffen. Anlaß für Kontroll- oder Informationsbesuche können eine Eingabe oder Veröffentlichung in der Presse sein, ich führe sie aber auch ohne konkreten Anlaß durch. Im Regelfall erfolgt zuvor eine Anmeldung, insbesondere dann, wenn eine umfangreiche Vorbereitung erforderlich ist und dazu Unterlagen der zu kontrollierenden Stelle notwendig sind. Kontrollbesuche werden aber auch unangemeldet vorgenommen, besonders dann, wenn es darum geht, einen bestimmten Sachverhalt möglichst rasch aufzuklären.

2.2 Einzelne Kontroll- und Informationsbesuche

Ein Schwerpunkt meiner bisherigen Kontrolltätigkeit war die Region Franken. In dieser Region führten wir bei den Bürgermeisterämtern Bad Friedrichshall, Beilstein und Cleebronn, dem Regionalen Rechenzentrum Franken, dem Staatlichen Gesundheitsamt Heilbronn und der Polizeidirektion Heilbronn Kontrollbesuche durch. Ausschlaggebend für diese Konzentration auf einen in seiner Größe überschaubaren Raum war die damit gebotene Möglichkeit, den Datenaustausch zwischen verschiedenen Stellen mit unterschiedlichen Aufgaben zu beobachten.

Neben der Kontrolle von Behörden mit unterschiedlichen Aufgaben derselben Region kontrollierten wir im ganzen Land einige Behörden und Stellen mit teils gleichartigen, teils unterschiedlichen Aufgaben, nämlich

- die staatlichen Gesundheitsämter Heilbronn, Mannheim, Rottweil und Tübingen
- das Regionale Rechenzentrum Franken, die Rechenzentren der Oberfinanzdirektion Stuttgart und der Universität Mannheim
- die Universität Mannheim.

Gezielte Kontrollen fanden bei den Landratsämtern Enzkreis, Esslingen, Ludwigsburg und Tübingen, bei den Bürgermeisterämtern Mühlacker, Pforzheim und Stuttgart, beim Landeskriminalamt, bei der Landestierärztekammer Baden-Württemberg und bei der Württembergischen Gebäudebrandversicherungsanstalt statt.

Informationsbesuche machten wir beim Statistischen Landesamt, beim Landeskriminalamt, beim Landesamt für Verfassungsschutz, bei der Staatsanwaltschaft Stuttgart, bei der Stadt Karlsruhe, beim Regionalen Rechenzentrum Karlsruhe und bei der Oberfinanzdirektion Freiburg.

2.3 Konsequenzen

Wegen des umfassenden Anwendungsbereichs des Landesdatenschutzgesetzes konnte auch der größte Optimist nicht erwarten, daß die Verwaltungspraxis dieses Gesetz ohne Anpassungsschwierigkeiten vollzieht. Dies stellte ich bei meiner Kontrolltätigkeit in Rechnung. Es kam mir deshalb in erster Linie darauf an, den kontrollierten Stellen Hinweise zu geben, sie auf Mängel aufmerksam zu machen und sie zu beraten. Im Vordergrund stand das Ziel, im Weg der Zusammenarbeit den datenschutzrechtlichen Bestimmungen Geltung zu verschaffen. Ich machte deshalb bislang von meinem Recht, Verstöße gegen Datenschutzbestimmungen oder sonstige Mängel bei der Datenverarbeitung zu beanstanden, nur dann Gebrauch, wenn es sich um offensichtliche, schwerwiegende Verstöße handelte.

3. Beratungstätigkeit

3.1 Allgemeines

Eine wesentliche Ergänzung meiner Kontrollaufgaben ist meine Beratungstätigkeit. Durch sie kann ich präventiv tätig sein und von vornherein verhindern, daß Verstöße gegen Datenschutzbestimmungen vorkommen. Ich messe dieser Arbeit eine ganz erhebliche Bedeutung zu. Deshalb teilte ich schon unmittelbar nach Übernahme meines Amtes den Ministerien meine Bereitschaft mit, diese Beratung wahrzunehmen. Leider entsprachen lediglich das Ministerium für Kultus und Sport und das Ministerium für Ernährung, Landwirtschaft, Umwelt und Forsten

meiner Bitte, die nachgeordneten Behörden über mein Beratungsangebot zu informieren. Die anderen Ressorts beschränkten sich auf den Hinweis, daß ich nach § 16 LDSG die Behörden beraten könne. Das Finanzministerium und das Ministerium für Ernährung, Landwirtschaft, Umwelt und Forsten wiesen zusätzlich ihre Behörden an, ihnen jede Inanspruchnahme meiner Dienststelle für Beratungszwecke mitzuteilen. Dadurch verdrehten sie mein Anliegen ins Gegenteil. Ich kann mir diese für die Behörden nicht gerade ermunternde Haltung der Ministerien nur aus Unsicherheit über das neugeschaffene Amt des Landesbeauftragten für den Datenschutz erklären. Insgesamt kann ich jedoch feststellen, daß inzwischen mein Rat schon oft eingeholt wurde. Vor allem gilt dies für die Behörden der unteren Verwaltungsebene, die in erster Linie das Datenschutzrecht in die Praxis umsetzen müssen und daher laufend mit datenschutzrechtlichen Problemen konfrontiert sind.

3.2 Einzelne Beratungen

Im besonderen Maße ließen sich die Meldebehörden beraten. Sie haben offensichtlich erhebliche Probleme mit der Anwendung der durch das Landesdatenschutzgesetz gefaßten Bestimmungen über die Erteilung von Auskünften aus dem Melderegister. Zahlreiche Anfragen kamen aber auch aus dem Schulbereich; dort warf das Landesdatenschutzgesetz eine Reihe von Zweifelsfragen auf. Einige Stellen wenden sich bereits laufend an mich, so daß schon von einer Dauerberatung gesprochen werden kann. Vereinzelt baten inzwischen auch schon Ministerien, z. B. Innenministerium, Finanzministerium und Sozialministerium um meine Beratung.

3.3 Mitwirkung an der Gesetzgebung

Der Bundestag verabschiedete in den letzten Monaten zwei für den Datenschutz besonders bedeutsame Bundesgesetze: das Melderechtsrahmengesetz und das Sozialgesetzbuch (SGB) — Verwaltungsverfahren —, in dem eine umfassende Regelung des Schutzes der Sozialdaten im Anwendungsbereich des Sozialgesetzbuchs enthalten ist. Während der Beratung dieser Gesetze im Bundesrat wandte ich mich mit Stellungnahmen und Vorschlägen an die Landesregierung, um im Interesse des Datenschutzes notwendig erscheinende Lösungen zu erreichen. Erfreulicherweise folgte die Landesregierung in beiden Fällen im wesentlichen meinen Vorstellungen und nahm eine entsprechende Haltung im Bundesrat ein.

3.4 Expertenkommission „Neue Medien“

Der von der Landesregierung eingesetzten Expertenkommission „Neue Medien“ gehöre ich als ständiger Beobachter an. Dieser Aufgabe messe ich besondere Bedeutung zu, weil die neuen Medien eine Reihe neuartiger und schwieriger Datenschutzprobleme aufwerfen. Im Rahmen dieser Tätigkeit erstattete ich der Expertenkommission ein Gutachten zu den datenschutzrechtlichen Problemen der neuen Medien.

4. Datenschutzregister

4.1 Sinn und Zweck

Das Landesdatenschutzgesetz beauftragte mich, ein Register aller Dateien mit personenbezogenen Daten zu führen. Dieses Register hat verschiedene Aufgaben. Die wichtigste sehe ich in der Information des Bürgers. Mit Hilfe des Datenschutzregisters kann der einzelne zwar nicht feststellen, ob und welche Daten

über ihn in Dateien gespeichert sind. Er kann aber daraus entnehmen, wo und welche Daten über ihn gespeichert sein könnten. Weiß er dies, kann er sein Auskunftsrecht geltend machen und bei den einzelnen Behörden konkret nachfragen. Auf diese Weise erfährt er dann, welche Stellen über ihn Daten vorhalten. Damit trägt das Datenschutzregister auch zu einer Transparenz der Datenverarbeitung bei. Diese Transparenz kommt nicht nur dem einzelnen Bürger, der in das Datenschutzregister Einsicht nehmen kann, zugute, sondern auch z. B. der Öffentlichkeit, dem Parlament, der Regierung und der gesamten Verwaltung. Schließlich ist das Datenschutzregister ein wesentliches Hilfsmittel für die Wahrnehmung meiner Aufgaben.

4.2 Datenschutzregisterverordnung

Das Landesdatenschutzgesetz legt nur fest, welche Stellen welche Dateien zum Register melden. Nicht abschließend regelt es die mitteilungsrechtlichen Angaben und das Mitteilungsverfahren. Diese Fragen soll das Innenministerium in einer Rechtsverordnung entscheiden. Leider steht diese Rechtsverordnung noch immer aus. Dies müßte nicht sein, denn die Ermächtigung zum Erlass der Verordnung, die ohnehin nur wenige Paragraphen umfassen wird, ist bereits seit Ende 1979 in Kraft. Obwohl ich das Datenschutzregister zu führen habe und es vor allem auch meine Arbeit erleichtern soll, erhielt ich erst nach längerem Drängen im Juni 1980 einen Verordnungsentwurf zur Stellungnahme. Unter Berücksichtigung der Erfahrungen, die andere Länder mit dem Aufbau des Datenschutzregisters machten, schlug ich dabei vor, daß die Behörden ihre Mitteilungen zum Datenschutzregister mir unmittelbar zuleiten. Damit wollte ich sicherstellen, daß

- die Mitteilungen der Wirklichkeit entsprechen,
- die Verantwortlichkeit der die Datei führenden Stelle uneingeschränkt gewahrt bleibt,
- kein unnötiger Verwaltungsaufwand entsteht, wie es bei dem von den Ressorts angestrebten Meldeweg aller Landesbehörden über ihre Ministerien unausweichlich der Fall ist,
- ich in direkten Kontakt mit möglichst vielen meiner Kontrolle unterliegenden Behörden treten kann.

Da die Ressorts ihre Fach- und Rechtsaufsicht höher bewerten als meine Überlegungen, steht zu befürchten, daß meinem Vorschlag nicht gefolgt wird.

4.3 Aufbau des Datenschutzregisters

Die Anlegung des Datenschutzregisters setzt die Datenschutzregisterverordnung voraus, da erst dann feststeht, welche Mitteilungen zu machen sind. Bis zu diesem Zeitpunkt kann ich lediglich die notwendigen organisatorischen Vorbereitungen treffen. Dies habe ich getan. So erarbeitete ich z. B. einen Mustervordruck für die Mitteilungen zum Datenschutzregister und stimmte diesen mit den Ministerien und kommunalen Landesverbänden ab. Ich werde dieses Muster bekanntgeben, sobald die Datenschutzregisterverordnung verkündet ist. Je länger sich dieser Zeitpunkt verzögert, um so wahrscheinlicher wird es allerdings, daß das Datenschutzregister nicht bis zu dem im Landesdatenschutzgesetz vorgesehenen Zeitpunkt, nämlich dem 29. Juni 1981, angelegt sein kann. Dies bedaure ich ebenso wie die Tatsache, daß wegen der bisherigen Verzögerungen beim Erlass der Datenschutzregisterverordnung die Behörden ihrer seit Ende September bestehenden Gesetzspflicht nicht nachkommen können, mir neu von ihnen eingerichtete Dateien zu melden.

5. Öffentlichkeitsarbeit

Die Wirksamkeit des Datenschutzes hängt wesentlich davon ab, ob die Bürger bereit und in der Lage sind, ihre Rechte geltend zu machen. Dazu bedarf es der Information. Wichtig ist, bei Bürger und Verwaltung Verständnis für den Datenschutz zu wecken, Probleme aufzuzeigen und auf Möglichkeiten und Grenzen des Datenschutzes hinzuweisen. Ich bemühe mich, dies im Rahmen meiner Möglichkeiten zu tun. Das Echo, das ich fand, ist ermutigend.

5.1 Informationsblatt „Datenschutz — Chance und Aufgabe“

Eine große Breitenwirkung konnte ich mit meinem Informationsblatt erzielen. Dieses Faltblatt schildert die wichtigsten Regelungen des Landesdatenschutzgesetzes, macht die Bürger auf ihre Rechte aufmerksam und beschreibt meine Aufgaben. Bereits einen Monat nach Erscheinen waren 40 000 Stück der 1. Auflage von 64 000 Exemplaren ausgegeben. Die Nachfrage nach diesem Informationsblatt hält unvermindert an. Bei der Verteilung unterstützten mich viele Stellen tatkräftig. Lediglich das Finanzministerium lehnte ab, das Faltblatt bei den Finanzämtern auszulegen, weil es glaubt, die Information trage den Gegebenheiten der Steuerverwaltung nicht in ausreichendem Maße Rechnung.

5.2 Veröffentlichungen und Vorträge

Neben dieser allgemeinen Information habe ich mich bemüht, in Kontakten mit Presse, Funk und Fernsehen und durch Teilnahme an Vortrags- und Diskussionsveranstaltungen Verständnis für den Datenschutz zu wecken, zu einzelnen datenschutzrechtlichen Problemen Stellung zu nehmen und die Öffentlichkeit über von mir untersuchte Vorgänge zu informieren.

5.3 Fortbildung

Die Fortbildung der Angehörigen der Verwaltung in Fragen des Datenschutzes halte ich für sehr wichtig. Mitarbeiter von mir wirkten deshalb bereits an verschiedenen Fortbildungsveranstaltungen mit. Ich habe die Absicht, diese Aktivitäten zu verstärken.

3. Teil: Schwerpunkte der bisherigen Tätigkeit

1. Abschnitt: Öffentliche Sicherheit und Ordnung

1. Polizei

1.1 Polizeiliche Informations- und Auskunftssysteme

Wichtige Instrumente polizeilicher Arbeit sind die elektronischen Informationssysteme.

1.1.1 INPOL-Neuordnung

Die Polizeien der Länder und des Bundes wollen ihr gemeinsames Informations- und Auskunftssystem für die gesamte Polizei (INPOL) in wesentlichen Teilen neu ordnen. Bausteine dieses Systems sind die Personenfahndung, Sachfahndung, Haftdatei, Straftaten/Straftäterdatei, Daktyloskopie und die Zentrale Fundstellendokumentation in umfangreichen Ermittlungskomplexen (PIOS). Den Zugang zu diesem System erschließt ein Personenindex. Ziel der

gegenwärtigen Bestrebungen ist, entgegen dem ursprünglichen Konzept vor allem dessen Datenumfang einzugrenzen. Bund und Länder haben deshalb ein erstes Konzept für Aufbau und Führung des sog. Kriminallaktennachweises (KAN) vorgelegt. Wie die endgültige Lösung aussehen wird, läßt sich wegen der zum Teil stark divergierenden Meinungen derzeit nicht absehen. Im Vordergrund der Überlegungen stehen folgende Probleme:

- Speicherung aller Daten in einer Datenverarbeitungsanlage.

Nach dem Konzept sollen alle Daten beim Bundeskriminalamt in der Weise gespeichert werden, daß die Daten der regionalen Straftäter in regionalen Kriminalaktennachweisen, die der überregionalen Straftäter in einem zentralen Kriminalaktennachweis gespeichert werden. Die verschiedenen Datenbestände sollen in einem Rechenzentrum geführt und nur durch ein Sperrkennzeichen voneinander unterschieden werden.

Dies garantiert nach meiner Auffassung keine vollständige Sicherung vor unbefugter Verwertung, weil über alle Daten durch ein Programm und einen Zugriff verfügt werden kann. Die Konsequenz aus der begrüßenswerten Unterscheidung zwischen regionalen und überregionalen Straftätern wird im technischen Bereich unbefriedigend realisiert. Dem Datenschutz wäre am besten Rechnung getragen, wenn die verschiedenen Datenbestände völlig getrennt in verschiedenen Datenverarbeitungsanlagen gespeichert würden, und zwar die Daten des zentralen KAN beim Bundeskriminalamt und die des regionalen KAN bei den Landeskriminalämtern.

- Umfang der im KAN gespeicherten Daten

Nach dem Konzept sollen außer den Personalien des Bürgers und dem Aktennachweis u. a. Haftnotierungen über richterlich angeordnete Freiheitsentziehungen sowie alle Straftaten erfaßt werden.

Dies zeigt, daß der Kriminalaktennachweis wesentlich weiter geht als seine Bezeichnung vermuten läßt. Über den reinen Aktennachweis hinausgehende Daten sollten nur aufgenommen werden, soweit es unter Abwägung des Interesses an einer wirksamen Verbrechensbekämpfung und den Aspekten des Datenschutzes dringend erforderlich ist. Man sollte deshalb nur aktuelle Haftnotierungen speichern. Gegen die Speicherung inaktueller Haftdaten bestehen insbesondere dann Bedenken, wenn der für die Anordnung der Untersuchungshaft erforderliche dringende Tatverdacht weggefallen ist. Auch muß die Notwendigkeit der Speicherung von Straftaten noch eingehend geprüft werden. Sie kann auf alle Fälle nur hingenommen werden, wenn Straftaten von rein örtlicher Bedeutung ausgenommen werden und im übrigen eine laufende Bestandsbereinigung aufgrund der Entscheidungen der Justiz sichergestellt ist.

- Umfang der im zentralen KAN gespeicherten Daten

Im zentralen KAN sollen die Daten aller Personen gespeichert werden, die erkennungsdienstlich behandelt wurden. Angesichts der geringen gesetzlichen Voraussetzungen für erkennungsdienstliche Maßnahmen sehe

ich hierfür keine Notwendigkeit. Auch vermag eine erkennungsdienstliche Behandlung noch keine überregionale Bedeutung zu begründen.

— Abgrenzung zwischen regionalem und zentralem KAN

Nach dem Konzept soll der polizeiliche Sachbearbeiter entscheiden, ob er Daten in den zentralen oder regionalen KAN eingibt. Maßgeblich sollen Schwere, Art und Umstände der Tat sowie die Wahrscheinlichkeit der Wiederholung von Straftaten an anderen Orten sein. Eine derartige Prognose ist schwierig. Es besteht die Gefahr, daß Daten im Zweifel in den zentralen KAN eingegeben werden. Eine Präzisierung z. B. nach Art der Straftat und Tat Umständen ist deshalb dringend erforderlich.

— Zusammenführung der Daten

Nach dem Konzept kann die Polizei bei Eingaben in den regionalen KAN durch technische Vorkehrungen bewirken, daß im Falle weiterer Eingaben in einen anderen regionalen oder den zentralen KAN die Daten entweder im regionalen KAN bleiben oder automatisch in den zentralen KAN überführt werden.

Ich meine, daß Daten allenfalls bei Eingabe weiterer Daten in den zentralen KAN automatisch übertragen werden können. Im übrigen sind die Daten durch Entscheidung im Einzelfall zusammenzuführen.

— Auskunftserteilung durch das Bundeskriminalamt

Das Bundeskriminalamt soll zur Erfüllung seiner Auskunftsverpflichtungen gegenüber dem Bürger zur Nachfrage im gesamten KAN berechtigt sein.

Dies ist nicht erforderlich, da Auskünfte aus den regionalen Kriminalaktennachweisen von den aktenführenden Dienststellen der Länder erteilt werden.

— Automatische Fortschreibung der Aussonderungsfrist im regionalen KAN

Die Lösungsfristen sollen nach dem Konzept nur im zentralen KAN automatisch fortgeschrieben werden. Dies halte ich nicht für ausreichend.

Ich hoffe und werde mich dafür einsetzen, daß im Verlauf der weiteren Beratungen das KAN-Konzept in der von mir aufgezeigten Richtung verbessert wird.

1.1.2 Personenauskunftsdatei des Landes (PAD)

Das Landeskriminalamt unterhält für die Polizeidienststellen des Landes ein Informationssystem, in dem alle zur Verbrechensbekämpfung wichtigen Daten über Straftäter und die von ihnen begangenen Straftaten gespeichert sind: die sogenannte Personenauskunftsdatei (PAD). Erfasst werden alle Straftaten mit Ausnahme bestimmter Verkehrsstraftaten. Verantwortlich für Richtigkeit und Vollständigkeit der gespeicherten Daten ist jeweils die zuständige örtliche Polizeidienststelle, die über eine eigene Datenstation verfügt. Die Sperrung einzelner Daten ist gegenwärtig nicht möglich. Löschungen werden ganz überwiegend auf Antrag von Bürgern und nur selten von Amts wegen

durchgeführt, obwohl nach der Dienstanweisung Datensätze zu löschen sind,

- wenn die zuständige Landespolizeidirektion einen Löschungsantrag stellt,
- wenn die Eingabe aufgrund einer falschen Anschuldigung erfolgte,
- wenn kein polizeiliches Interesse an der weiteren Speicherung besteht oder das Verfahren aufgrund erwiesener Unschuld eingestellt wurde.

Für die restriktive Handhabung sind folgende Gründe maßgeblich:

- Regelaussonderungen finden nicht statt, da erst das Inkrafttreten der Richtlinien für die Führung kriminalpolizeilicher Sammlungen (KpS-Richtlinien) abgewartet werden soll.
- Einzelaussonderungen von Amts wegen erfolgen häufig deshalb nicht, weil der Polizei der Ausgang des Ermittlungs- oder Strafverfahrens nicht bzw. nicht genau bekannt ist. Dies wiederum ist darauf zurückzuführen, daß die Justiz die Polizei nicht in allen Fällen, wie es an sich die Anordnung über die Mitteilungen in Strafsachen vorsieht, über den Ausgang des Verfahrens unterrichtet. Auch ist der Inhalt der Mitteilungen zu undifferenziert. Ihnen läßt sich beispielsweise nicht entnehmen, aus welchen Gründen ein Verfahren eingestellt worden ist. Davon hängt jedoch mitunter die Beurteilung ab, ob Daten zur weiteren Aufgabenerfüllung der Polizei noch erforderlich sind.

Bei PAD müssen folgende Punkte vordringlich geprüft bzw. geändert werden:

- Umfang der gespeicherten Daten

Die Erforderlichkeit der Datenspeicherung ist in zweifacher Hinsicht zu überprüfen: Zum einen ist zu untersuchen, ob nahezu alle Straftäter in der zentralen Datei des Landes gespeichert sein müssen. Was im Verhältnis zwischen Bund und Ländern gilt, muß in gleicher Weise für die Verhältnisse innerhalb des Landes gelten. Von der Speicherung oder zumindest der zentralen Speicherung könnten möglicherweise Bagatelldelikte, so etwa bestimmte Privatklagedelikte oder einzelne Delikte des Nebenstrafrechts ausgenommen werden. Zum andern ist zu prüfen, ob bei zulässiger Datenspeicherung es in jedem Falle erforderlich ist, alle derzeit vorgesehenen Einzeldaten zu erheben und zu speichern.

- Sperrung und Löschung von Daten

Die Praxis der Sperrung und Löschung von Daten entspricht derzeit nicht § 13 LDSG. Ich wies deshalb das Innenministerium nachdrücklich darauf hin, daß eine gesetzmäßige Handhabung kurzfristig herbeigeführt werden muß. In diesem Rahmen muß das Innenministerium auch dafür sorgen, daß der Ausgang der Ermittlungs- bzw. Strafverfahren bei der Frage der weiteren Datenspeicherung gebührend berücksichtigt wird. Das Justizministerium wird hierfür die Voraussetzungen schaffen und das Mitteilungsverfahren verbessern müssen.

— Auskunftserteilung an Bürger

Derzeit erteilt das Landeskriminalamt Auskünfte an Bürger. Nach dem Landesdatenschutzgesetz ist es hierfür nicht zuständig, da es nicht selbst speichernde Stelle ist. Um die jetzige durchaus zweckmäßige Praxis beibehalten zu können, sollte eine einwandfreie Rechtsgrundlage geschaffen werden.

1.1.3 Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien)

Die Polizeien der Länder und des Bundes erarbeiteten unter maßgeblicher Beteiligung aller Datenschutzbeauftragten den Entwurf von Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen. Sein Inhalt ist:

- Er konkretisiert die Regeln der Datenschutzgesetze über die Speicherung und Löschung bzw. Aussonderung von Daten in sog. kriminalpolizeilichen personenbezogenen Sammlungen und die Übermittlung hieraus. Dabei ist gleichgültig, ob diese Daten in Form von Akten oder Dateien geführt werden.
- Besonders bedeutsam ist, daß die Aufbewahrungsdauer kriminalpolizeilicher Unterlagen beschränkt wird:
 - Die Unterlagen sind regelmäßig auszusondern, wenn beim Betroffenen die Voraussetzungen für eine Aufnahme von Erkenntnissen in die kriminalpolizeiliche Sammlung 10 Jahre zurückliegen, jedoch nicht vor Ablauf von 10 Jahren nach der Entlassung aus einer Justizvollzugsanstalt oder nach Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung, ferner, wenn der Betroffene das 70. Lebensjahr vollendet hat, es sei denn, daß er in den zurückliegenden 5 Jahren die Voraussetzungen für die Aufnahme von Erkenntnissen in die Sammlung erfüllte.
 - Sonderregelungen wurden — nicht zuletzt auch aufgrund meiner Bemühungen — für Kinder und Jugendliche gefunden, deren personenbezogene Daten nach Auffassung der Polizei ebenfalls in den kriminalpolizeilichen Sammlungen gespeichert werden müssen. So ist bei Kindern spätestens nach 2 Jahren, bei Jugendlichen spätestens nach 5 Jahren zu prüfen, ob eine Aussonderung möglich ist. Darüber muß die Polizei grundsätzlich die Sorgeberechtigten unterrichten, wenn sie Unterlagen über Kinder in die kriminalpolizeilichen Sammlungen aufnimmt.
 - Abkürzungen der Regelfristen in Fällen geringerer Bedeutung sind ebenso möglich wie Verlängerungen, vor allem bei bestehender Wiederholungsgefahr.
 - Aussonderungen sind ferner vorzunehmen, wenn die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergeben, daß die Gründe, die zur Aufnahme in die kriminalpolizeiliche Sammlung geführt haben, nicht zutreffen.

1.1.4 Richtlinien für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt (Dateien-Richtlinien)

Der Bundesminister des Innern hat den Entwurf von Richtlinien für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt (Dateien-Richtlinien) vorgelegt. Diese Richtlinien berühren die Polizeien der Länder stark, weil sie für die meisten Dateien die Daten anliefern. Die Richtlinien sollen Kriterien für die Erhebung, Speicherung, Übermittlung und Löschung von Daten festlegen. Jede einzelne beim Bundeskriminalamt geführte Datei soll an diesen Grundsätzen gemessen werden. Aus der Fülle der damit verbundenen Probleme möchte ich nur wenige herausgreifen:

— Speichernde Stelle bei Verbunddateien

Die Datenschutzgesetze knüpfen zahlreiche Rechtsfolgen an den Begriff der speichernden Stelle. Darunter ist jede Behörde zu verstehen, die Daten für sich selbst speichert oder durch andere speichern läßt. Die speichernde Stelle muß über die Speicherung, Übermittlung, Sperrung und Löschung von Daten entscheiden; auch ist es ihre Sache, dem Bürger Auskünfte über gespeicherte Daten zu erteilen. Im Rahmen der Dateienrichtlinien stellt sich die Frage, wer speichernde Stelle der von den Ländern angelieferten Daten ist: die Polizeidienststellen der Länder und/oder das Bundeskriminalamt. Der Bundesminister des Innern und der Bundesbeauftragte für den Datenschutz leiten aus der im Grundgesetz und im Kriminalgesetz verankerten Zentralstelleneigenschaft des Bundeskriminalamts ab, diese Behörde sei für alle Daten, die in den bei ihr geführten Dateien enthalten sind, speichernde Stelle.

Ich vertrete hingegen die Auffassung und das Innenministerium ist mir darin gefolgt, daß die datenschutzrechtlichen Verpflichtungen die Stelle treffen müssen, die für die Erledigung der Sachaufgabe zuständig ist. Das sind aber nach der Kompetenzverteilung des Grundgesetzes im Regelfall die Polizeidienststellen der Länder. Bearbeiten sie einen Ermittlungsvorgang und geben sie die Daten in die Datenverarbeitungsanlage ein, so sind sie auch selbst speichernde Stellen und als solche für die Richtigkeit, Vollständigkeit, Sperrung und Löschung der Daten verantwortlich. Die gegenteilige Meinung würde es dem Bund erlauben, die Kontrolle für die polizeiliche Arbeit in den Ländern auszuüben.

— Auskunftserteilung bei Verbunddateien

Mit der vorstehenden Problematik eng verknüpft ist die Frage, wer dem Bürger auf Antrag Auskunft über die zu seiner Person gespeicherten Daten erteilt. Auskunft erteilende Stelle ist nach allen Datenschutzgesetzen die speichernde Stelle. Dies führt zu Problemen, wenn mehrere Länder — unter Umständen auch der Bund — über einen Bürger Daten in einer beim Bundeskriminalamt geführten Datei gespeichert haben. Die von dem Bürger um Auskunft ersuchte Stelle müßte ihre Auskunft auf die von ihr selbst eingegebenen Daten beschränken, zugleich aber mitteilen, daß andere Stellen ebenfalls Daten gespeichert haben. Dies hätte Nachteile für die Bür-

ger, unter Umständen aber auch für die Polizei. Der Bürger wäre gezwungen, bei einer Vielzahl von Polizeidienststellen nachzufragen, ob dort Daten über ihn gespeichert sind. Interessen der Polizei könnten beeinträchtigt werden, wenn der Bürger erfährt, daß andere Polizeidienststellen weitere Daten über ihn speichern.

Die Dateien-Richtlinien stellen es in das Ermessen des Bundeskriminalamts, ob es einen Auskunftsantrag selbst bescheidet oder ob es diesen an die datenanliefernde Polizeidienststelle oder im Falle mehrerer datenanliefernder Verbundteilnehmer an das Land abgibt, in dem der Betroffene seinen Wohnsitz hat. Eine rechtlich befriedigende Lösung ist auch dies nicht. Längerfristig wäre eine Regelung dahin wünschenswert, welche die Auskunftserteilung im Bereich der Polizei einer Stelle — etwa der Behörde/Dienststelle am Wohnsitz des Betroffenen — überträgt.

— Speicherung von Daten über nicht verdächtige oder beschuldigte Personen

- Nach den Dateien-Richtlinien sollen — unbeschadet der Eingrenzung, die sich aus dem Zweck der jeweiligen Datei und der Erforderlichkeit der Datenspeicherung zur Aufgabenerfüllung ergibt — auch Angaben über gefährdete Personen, Anzeigeerstatte, Hinweisgeber, Zeugen und Geschädigte gespeichert werden. Ich habe erhebliche Zweifel, ob Daten dieses Personenkreises ohne Einwilligung der Betroffenen beim Bundeskriminalamt gespeichert werden dürfen.
- Nach den Richtlinien sollen unter Umständen nicht verdächtige Personen allein deshalb gespeichert werden, weil zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Strafen oder zur Ergreifung von zur Festnahme gesuchten Personen erforderlich ist. Die Betroffenen sollten über die Tatsache der Speicherung unterrichtet werden, sobald die Dauer der Speicherung ein Jahr überschritten hat.

Zweifelhaft ist, ob Daten dieser Personen aufgrund der §§ 161, 163 der Strafprozeßordnung erhoben und zur Erfüllung von Strafverfolgungsaufgaben gespeichert werden dürfen. Bedenken habe ich dagegen, daß die Daten von nicht verdächtigen oder beschuldigten Personen immer schon dann gespeichert werden, wenn dies zur Ergreifung von zur Festnahme gesuchter Personen erforderlich ist. Hält man eine Datenspeicherung auch in diesem Falle für zulässig, so sollte wenigstens eine nachträgliche Unterrichtung des Betroffenen erfolgen, wenn eine Gefährdung des mit der Speicherung verbundenen Zwecks ausgeschlossen werden kann (vgl. hierzu auch § 5 des Gesetzes zu Artikel 10 des Grundgesetzes). Nur bei kurzzeitiger Speicherung sollte man hiervon absehen.

1.1.5 Vereinfachtes Verfahren zur Bearbeitung von Bagatelldelikten

Das Polizeipräsidium Karlsruhe und die Polizeidirektion Ravensburg erproben seit etwa 1½ Jahren ein vereinfachtes Verfahren zur Bearbeitung von Bagatelldelikten. Ange-

wandt wird es hauptsächlich bei Privatklagedelikten (z. B. Beleidigung, Körperverletzung, Sachbeschädigung) und Offizialdelikten (z. B. Diebstahl), soweit der Objektwert oder Schadensumfang gering und der Fall tatsächlich und rechtlich einfach gelagert ist. Für die Bearbeitung der Anzeigen wird ein Formular verwandt. Die Delikte sind je nach Gewichtung des Straftatbestandes und der Höhe des Objektwertes/Schadensumfanges in zwei Fallgruppen unterteilt. Durch diese Unterteilung werden Art und Umfang der polizeilichen Ermittlungstätigkeit sowie die aktenmäßige Erfassung des Sachverhalts bestimmt. Bei der ersten Fallgruppe fertigt die Polizei keine Vernehmungsniederschriften von Zeugen und Beschuldigten, es sei denn, der Beschuldigte will sich äußern. Auch behandelt sie Ermittlungsvorgänge gegen Kinder immer nach der ersten Fallgruppe. Verfahren gegen Jugendliche und Heranwachsende werden in herkömmlicher Weise bearbeitet.

Datenschutzrechtliche Aspekte spielen bei diesem Verfahren eine Rolle, weil die Polizei die Daten aufgrund der Anzeige in PAD speichert. Meine Bedenken richten sich vor allem gegen folgendes:

- Es ist zwar verständlich, daß Justiz und Polizei angesichts der ständig steigenden Zahl der Straftaten nach neuen Wegen für die Bearbeitung von Bagatelldelikten suchen. Es stellt sich jedoch — von der grundsätzlichen Problematik der Erfassung einmal abgesehen — die Frage, ob der Ermittlungsumfang und die aktenmäßige Erfassung nicht so sehr eingeschränkt wird, daß die Polizei keine ausreichende Beurteilungsgrundlage mehr dafür hat, ob die Speicherung der Daten des Betroffenen in der Personenauskunftsdatei zur Erfüllung polizeilicher Aufgaben erforderlich ist. Dies gilt insbesondere in den Fällen, in denen von einer Vernehmung des Beschuldigten und der Zeugen abgesehen werden kann.
- Erst recht stößt die vereinfachte Bearbeitung von Anzeigen gegen Kinder auf Bedenken. Solange auf eine Speicherung der Daten von Kindern in der PAD nicht verzichtet wird, ist eine sorgfältige Sachaufklärung erforderlich. Nur so wird den Besonderheiten in diesem Bereich Rechnung getragen.
- Meine Bedenken verstärken sich dadurch, das sich die eingeschränkte Ermittlungstätigkeit der Polizei auf die Entscheidungen der Staatsanwaltschaft auswirkt. Häufig wird die Einstellung des Verfahrens feststehen, jedoch nicht der genaue Einstellungsgrund. Dies kann dazu führen, daß die Daten weiter in PAD gespeichert sind, obwohl sie nach dem Landesdatenschutzgesetz zumindest gesperrt werden müßten.

1.2 Probleme der polizeilichen Praxis in Baden-Württemberg

1.2.1 INPOL-Abfrage bei Zeugen und Anzeigerstattem

Das Innenministerium wies 1977 die Polizeidienststellen an, im Wege einer sogenannten INPOL-Abfrage Personen zu überprüfen, die der Polizei bei der Erfüllung ihrer Aufgaben namentlich bekannt werden. Abgesehen werden soll davon lediglich in einigen wenigen Fällen. Die Anordnung geht auf eine — inzwischen auch in der Presse erwähnte — Empfehlung der Innenministerkonferenz zurück. Gegen

diese Regelung äußerte ich gegenüber dem Innenministerium Bedenken:

Die Datenabfrage mag zwar zweckmäßig sein, da auf diese Weise auch einmal ein gesuchter Straftäter erkannt werden kann. Ich halte sie jedoch — sofern das Verhalten des Bürgers nicht zu weiteren Nachforschungen Anlaß gibt — nicht für geboten; denn die Polizei hat im Zeitpunkt der Abfrage keine sachlich einleuchtende Begründung für deren Notwendigkeit. Kein Verständnis habe ich dafür, daß nach dem Erlaß der Bürger selbst dann als potentieller Rechtsbrecher betrachtet wird, wenn er die Polizei — wie etwa als Zeuge oder Anzeigerstatter — unterstützen will. Dies widerspricht nach der Rechtsprechung des Bundesverwaltungsgerichts dem Menschenbild des Grundgesetzes. Ich meine, die Polizei sollte — nicht zuletzt auch im Interesse eines guten Verhältnisses zum Bürger — künftig von einer generellen Überprüfung nicht verdächtiger oder beschuldigter Personen absehen. Eine INPOL-Abfrage sollte allenfalls dann durchgeführt werden, wenn die Voraussetzungen für eine Identitätsfeststellung nach der Strafprozeßordnung oder dem Polizeigesetz gegeben sind. Ich hoffe, daß das Innenministerium dieser Empfehlung folgt.

1.2.2 Auskunftserteilung an Bürger

Nach § 12 Abs. 2 LDSG sind die Polizeidienststellen wie andere Sicherheitsbehörden nicht verpflichtet, einem Bürger auf Antrag Auskunft über seine etwa gespeicherten Daten zu geben. Der Wortlaut dieser Bestimmung bereitete der Polizei anfänglich Schwierigkeiten. Sie verstand sie mitunter als Auskunftsverbot. In Wirklichkeit besagt die Vorschrift, daß die Auskunftserteilung im Ermessen der jeweiligen Polizeidienststelle steht. Eine Auskunft ist dann zu erteilen, wenn eine Abwägung ergibt, daß das Interesse des Bürgers an der Auskunftserteilung das polizeiliche Interesse an der Geheimhaltung überwiegt. Die Erteilung einer Auskunft kommt vor allem in Betracht, wenn es sich um Unterlagen handelt, an deren Zustandekommen der Bürger selbst beteiligt war und von denen er den Umständen nach annehmen kann, daß sie die Polizei aufbewahrt.

Aufgrund einiger Eingaben von Bürgern, die die Polizeidienststellen vergeblich um Auskunft ersuchten, und Erörterungen mit Polizeidienststellen habe ich gewisse Zweifel, ob die Praxis diesen Grundsätzen bereits voll entspricht. Mir scheint die Polizei mitunter die Gefahr der Ausforschung durch die anfragenden Bürger zu hoch zu bewerten. Selbstverständlich kann niemand eine Ausforschung der polizeilichen Arbeit wollen. Nach meinen bisherigen Beobachtungen bezwecken die Auskunftersuchen jedoch anderes. So sind viele Bürger, die irgendwann einmal mit der Polizei in Berührung kamen, noch Jahre später über diesen Vorfall beunruhigt. Vor allem sie möchten, wie die Eingaben zeigen, von der Polizei ein offenes Wort hören. Ebenso häufig wünschen Bürger eine Auskunft, welche durch die öffentliche Diskussion der letzten Jahre über Sicherheitsfragen sensibilisiert oder verängstigt sind. Gerade hier würde die Polizei wesentlich zum Abbau von Mißtrauen gegen ihre Arbeit beitragen, wenn sie dem Bürger eine offene Auskunft erteilt. Ich rate jedem Bürger, der mich wegen einer Datenspeicherung bei der Polizei anspricht, der Polizei sein Auskunftersuchen zu

begründen und ihr dadurch die Auskunftserteilung zu erleichtern. Umgekehrt rate ich der Polizei, solche Auskunftsersuchen der Bürger nach Möglichkeit zu beantworten. In Einzelfällen ist es mir auch gelungen, die Polizei zu einer Änderung ihrer ablehnenden Haltung zu bewegen.

Im übrigen verweise ich bei jeder Gelegenheit auf die Möglichkeit, mich um Überprüfung zu bitten, wenn Anhaltspunkte für eine unzulässige Datenspeicherung bestehen. Ich habe das Recht, auf Eingaben von Bürgern hin bei der Polizei in vollem Umfang Dateiinhalte und dazugehörige Akten zu überprüfen. Vor allem für den Bürger, aber auch für mich ist jedoch unbefriedigend, daß ich nur das Ergebnis meiner Überprüfung in Form einer rechtlichen Beurteilung mitteilen darf, nicht auch, ob und welche Daten gespeichert sind.

1.2.3 Tagesberichte der Polizei

Polizeidienststellen auf Kreisebene übermitteln den Orts- und Kreispolizeibehörden regelmäßig sogenannte Tagesberichte. Darin sind die wichtigsten polizeilichen Ereignisse des Tages im Zuständigkeits- und Aufgabenbereich der Polizei abgehandelt. Die Tagesberichte enthalten eine Vielzahl personenbezogener und zum Teil hochsensibler Daten, die auf diese Weise eine breite Streuung erfahren. Begründet wird dies damit, daß die Polizeidienststellen nach dem Polizeigesetz die Orts- und Kreispolizeibehörden über sachdienliche Wahrnehmungen unterrichten müssen. Sachdienlich sind jedoch nur solche Wahrnehmungen, die Maßnahmen der Orts- oder Kreispolizeibehörden auslösen können. Dies gerade wird derzeit nicht durchweg beachtet. So erhalten z. B. die Ortspolizeibehörden häufig personenbezogene Daten von mutmaßlichen Straftätern mitgeteilt, obwohl in diesen Fällen in der Regel nur die Staatsanwaltschaft Entschließungen treffen wird. Ich habe daher eine Einschränkung dieser Praxis gefordert.

2. Verfassungsschutz

Das Bundesamt für Verfassungsschutz unterhält im Datenverbund eine Hinweisdatei für die Verfassungsschutzbehörden des Bundes und der Länder. Dieses nachrichtendienstliche Informationssystem (NADIS) enthält lediglich Personengrunddaten und Hinweise auf Aktenfundstellen. Diese geben den anfragenden Verfassungsschutzbehörden darüber Auskunft, ob und bei welcher Behörde Informationen über eine Person vorliegen.

Das Landesamt für Verfassungsschutz erließ inzwischen für NADIS Lösungsrichtlinien. Hiernach sind Datensätze grundsätzlich zu löschen, wenn sie über einen bestimmten Zeitraum hinweg nicht ergänzt wurden oder die Betroffenen ein bestimmtes Lebensalter erreicht haben. Vor jeder Datenspeicherung ist auch zu prüfen, ob die Regelfristen für deren Löschung abgekürzt werden können. Darüber hinaus hat der Sachbearbeiter während der laufenden Bearbeitung, insbesondere vor der Verwertung von Daten, zu prüfen, ob deren Speicherung noch erforderlich ist.

Das Landesamt für Verfassungsschutz erließ ferner eine Dienstweisung über die Führung von Arbeitskarteien. Hierin sind die Voraussetzungen für die Karteierfassung, Art und Inhalt der Karteien und deren Vernichtung geregelt.

Ich halte beide Regelungen für eine erhebliche Verbesserung des Datenschutzes. In Bälde werde ich mir ein Bild von ihrer Handhabung verschaffen.

3. Staatsanwaltschaften und Strafgerichtsbarkeit

Justiz und Polizei müssen auf dem Gebiet des Datenschutzes eng zusammenarbeiten, damit der Bürger vor Mißbrauch seiner persönlichen Daten geschützt wird. Wie wichtig diese Zusammenarbeit ist, zeigen die KpS-Richtlinien, die Dienstanweisung für die Personalauskunftsdatei und die Anordnung der Justiz über Mitteilungen in Strafsachen (MiStra) besonders deutlich.

3.1 Anordnung über Mitteilungen in Strafsachen

Die Justizverwaltungen der Länder und des Bundes vereinbarten vor Jahren die Anordnung über Mitteilungen in Strafsachen (MiStra). Auf ihrer Basis teilen seit langem Staatsanwaltschaften und Gerichte Entscheidungen im Ermittlungs- und Strafverfahren verschiedensten Behörden und Stellen mit, um sie über Vorgänge zu informieren, die für diese Anlaß zu Maßnahmen sein könnten. Diese Mitteilungen lösen nur in wenigen Fällen Maßnahmen der Verwaltungsbehörden aus; vielfach werden sie jedoch zu den Akten genommen. Die Anwendung der MiStra führt häufig zu einer globalen und schematischen Übermittlung besonders sensibler Daten, die eine Einzelfallprüfung unter Beachtung des Grundsatzes der Verhältnismäßigkeit vermissen läßt. Mit wenigen Ausnahmen besteht für die Datenübermittlung keine gesetzliche Grundlage.

Die Datenschutzbeauftragten der Länder und des Bundes vertreten unter Hinweis auf die Rechtsprechung des Bundesverfassungsgerichts übereinstimmend die Auffassung, daß Mitteilungen dieser Art und dieses Umfangs einen Eingriff in die nach Artikel 2 Abs. 1 des Grundgesetzes geschützte Rechtssphäre der Betroffenen darstellen und deshalb einer gesetzlichen Grundlage bedürfen. Ich fordere deshalb das Justizministerium auf, im Benehmen mit den Justizverwaltungen und den berührten Fachressorts der Länder und des Bundes die MiStra entweder so zu überarbeiten, daß nur noch Regelungen bestehen bleiben, für die eine Rechtsgrundlage vorhanden ist oder aber eine weitergehende gesetzliche Grundlage zu schaffen. In diesem Falle muß der Gesetzgeber die Voraussetzungen festlegen, unter denen Mitteilungen künftig zulässig sein sollen. Wichtig ist dabei auch, den Umfang der bisherigen Urteilsmitteilungen zu reduzieren. Mitunter wird es genügen, anstelle des vollständigen Urteils die Urteilsformel oder nur einen Teil hiervon mitzuteilen. In anderen Bereichen wiederum muß der Inhalt der Mitteilungen im Interesse des Betroffenen differenziert werden. Auch sollte die Anordnung der Mitteilung stärker als bisher in die Hand des Richters und des Staatsanwalts übergehen.

Zur Verdeutlichung der Problematik nenne ich einige besonders unbefriedigende Regelungen der MiStra:

— Mitteilungen an die Polizei

Nach den KpS-Richtlinien soll die Polizei in Zukunft Unterlagen aus kriminalpolizeilichen Akten aussondern, wenn ihre Ermittlungen oder eine ihr bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichts ergeben, daß die Gründe nicht zutreffen, die zur Aufnahme des Vorgangs in die Sammlung führten. Der Inhalt der Mitteilungen der Justiz nach der MiStra versetzt die Polizei jedoch nicht in die Lage, eine Entscheidung über die Aussonderung zu treffen. Sie kann dies nur, wenn sie den Grund für einen Freispruch oder die Einstellung eines Verfahrens möglichst genau erfährt.

Gegenwärtig müssen bestimmte Mitteilungen an das Bundeszentralregister zugleich auch an die Polizeidienststelle gehen,

in deren Bezirk der Wohnsitz des Beschuldigten liegt. Ich sehe keine Notwendigkeit, warum auf diese Weise ein Teil der Daten des Bundeszentralregisters zugleich auch noch dezentral gesammelt wird.

— Mitteilung zum Wählerverzeichnis

Nach der MiStra ist der Verwaltungsbehörde die Urteilsformel des Urteils mitzuteilen, durch das einem Bürger das Wahlrecht aberkannt wurde. Bei einer solchen Mitteilung könnte und sollte in Zukunft in der Regel auf die rechtliche Bezeichnung der Tat, deren der Verurteilte schuldig gesprochen wurde, auf das konkrete Strafmaß und die Anführung von Maßregeln der Sicherung und Besserung verzichtet werden.

— Mitteilungen in Strafsachen gegen Angehörige des öffentlichen Dienstes und anderer Berufsgruppen

Nach der MiStra müssen Entscheidungen der Justiz in Strafsachen gegen Angehörige des öffentlichen Dienstes, der Heilberufe und bestimmter Berufe des Wirtschaftslebens dem Dienstherrn oder den Aufsichtsbehörden oder den Berufskammern mitgeteilt werden. Ausgenommen sind lediglich Verkehrsstraftaten, es sei denn, daß es sich um schwerere Verstöße, namentlich um Vergehen der Trunkenheit im Straßenverkehr oder der fahrlässigen Tötung handelt. Ich halte es für wichtig, den Kreis der von der Mitteilungspflicht ausgenommenen Straftatbestände zu erweitern und stärker als bislang nach dem konkreten Tatvorwurf und der Funktion zu differenzieren, welche der Verurteilte in seinem Beruf wahrnimmt. Auch ist zu überlegen, ob zu den Akten genommene Mitteilungen nach bestimmten Fristen wieder entfernt werden können.

— Mitteilungen in Strafsachen gegen Studierende und Inhaber akademischer Grade

In Strafsachen gegen Studierende und Inhaber akademischer Grade sind rechtskräftige Entscheidungen mitzuteilen, durch die auf Freiheitsstrafe erkannt worden ist. Ich meine, diese Vorschrift sollte gestrichen werden.

— Mitteilungen an die Schule in Strafsachen gegen Jugendliche und Heranwachsende

In Strafsachen gegen Jugendliche und Heranwachsende sind nach §§ 70, 109 des Jugendgerichtsgesetzes Mitteilungen an die Schule nur in „geeigneten“ Fällen zu machen. Ich halte diesen Beurteilungsmaßstab für wenig hilfreich. Möglicherweise kann man auf eine derartige Unterrichtung, die auch als Disziplinierungsmittel dienen kann, ganz verzichten.

3.2 Zentrale Namenskartei bei den Staatsanwaltschaften

Die Staatsanwaltschaften führen ein zentrales Namensregister. Darin sind alle Personen eingetragen, gegen die ein Ermittlungsverfahren bei der Staatsanwaltschaft anhängig ist oder war. Üblicherweise werden Name, Vorname, Geburtstag und Anschrift des Betroffenen, Tatvorwurf, Name des Anzeigerstatters und Aktenzeichen des Verfahrens eingetragen. Die Kartei hat unterschiedliche Funktionen. Sie dient in erster Linie der Auffindung von Akten, beispielsweise der Zuordnung neu eingehender Vorgänge zu laufenden Verfahren oder der Zusammenführung mehrerer Verfahren. Auch ermöglicht sie, in zunächst abgeschlossenen, dann aber erneut aufgerollten Verfahren auf frühere Akten

zurückzugreifen. Bei neu eingehenden Anzeigen läßt sich über die Kartei feststellen, ob gegen den Beschuldigten bereits Verfahren anhängig waren. In solchen Fällen wird die Kartei zum Entscheidungsinstrument, wenn man auf das Beiziehen dieser Akten verzichtet. Schließlich gibt die Staatsanwaltschaft aus der Kartei auch Auskünfte an verschiedenste Stellen, z. B. an Vertreter des Beschuldigten, an Geschädigte, Gerichte, Polizei und Versicherungen. Geregelt ist bisher lediglich die Aufbewahrungsdauer der Karteikarten und der zugehörigen Akten. Sie ergibt sich aus den von Bund und Ländern beschlossenen Bestimmungen über Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden aus dem Jahre 1971.

Diese zentrale Namenskartei wirft eine Reihe von Datenschutzproblemen auf:

— Berichtigung von Daten

Daten sind zu berichtigen, wenn sie unrichtig sind. Diese Voraussetzungen liegen u. a. vor, wenn Staatsanwaltschaft oder Gericht von einem anderen Tatvorwurf als die Polizei ausgeht. Solange die Kartei als Entscheidungsinstrument dienen kann, ist die Berichtigung dieses Datums mehr als nur ein Formalakt.

— Sperrung bzw. Löschung von Daten

Daten sind zu sperren oder auf Antrag des Betroffenen auch zu löschen, wenn sie zur rechtmäßigen Aufgabenerfüllung nicht mehr benötigt werden. Ob diese Voraussetzungen vorliegen, ist wegen der unterschiedlichen Verwendungszwecke der Kartei nicht einfach festzustellen. Ich halte eine stärkere Differenzierung der Aufbewahrungsfristen für erforderlich, auch wenn ich nicht übersehe, daß sich dies wegen des Umfangs und der manuellen Führung der Namenskartei nicht einfach verwirklichen läßt. Vordringlich erscheint mir eine befriedigende Lösung für die Personen, deren Unschuld sich im Ermittlungs- oder Strafverfahren herausgestellt hat.

— Datenübermittlungen

Nach meinen Feststellungen erteilt die Staatsanwaltschaft aus der zentralen Namenskartei in größerem Umfang fernmündlich Auskünfte. Dies ist nur zulässig, wenn sie mit Sicherheit den Anrufer identifizieren kann.

4. Verkehrswesen

4.1 Erhebung personenbezogener Daten im Bußgeldverfahren

Im Bußgeldverfahren muß der Betroffene Gelegenheit haben, sich zu der Beschuldigung zu äußern. Dies erfolgt meist in der Weise, daß ihm ein Anhörungsbogen übersandt wird. Darin sind u. a. Fragen zur Person gestellt, die der Betroffene beantworten muß (§ 55 Abs. 1 OWiG i. V. m. § 136 Abs. 1 Satz 2 StPO). Welche Fragen zur Person gestellt werden dürfen, ergibt sich mittelbar aus § 111 des Ordnungswidrigkeitengesetzes. Allerdings dürfen nach Rechtsprechung und Literatur nur solche persönlichen Daten erhoben werden, die zur Feststellung der Identität der Betroffenen oder zur ordnungsgemäßen Erledigung staatlicher Aufgaben erforderlich sind. Dazu zählen die in dem Anhörungsbogen gestellten Fragen nach dem Beruf, dem Familienstand und dem Fernsprecher des Betroffenen in der Regel nicht. Ich schlug deshalb dem Innenministerium vor, auf diese

Angaben zu verzichten. Gleichzeitig regte ich an, auf den Bußgeldbescheiden künftig zu vermerken, ob eine Tat im Verkehrszentralregister eingetragen wird.

4.2 Bußgeldkarteien

Die Landratsämter und Bürgermeisterämter der Stadtkreise und Großen Kreisstädte führen in der Regel Bußgeldkarteien. In ihnen sind alle Verkehrssünder vermerkt, gegen die ein Bußgeldbescheid erlassen wurde. Der Inhalt dieser Karteien ist unterschiedlich: zum einen sind nur die Personalien des Bürgers und das Aktenzeichen des Bußgeldverfahrens eingetragen, zum andern jedoch auch der Tag des Erlasses des Bußgeldbescheides, der Tatvorwurf und die Höhe des Bußgeldbescheides. Die Behörden erteilen aus den zuerst genannten Karteien keine, aus den übrigen gelegentlich Auskünfte. Die Karteien dienen ihren Angaben nach vornehmlich Buchführungs-, Kassen- oder ähnlichen Zwecken. Die umfangreicheren Karteien ermöglichen es jedoch den Behörden, auch früher begangene Ordnungswidrigkeiten in einem neuen Bußgeldverfahren bei der Bemessung der Geldbuße erschwerend zu berücksichtigen.

Bei der datenschutzrechtlichen Beurteilung ist zu differenzieren: Die Karteien mit Grunddaten des Betroffenen und dem Aktenzeichen sind datenschutzrechtlich unbedenklich, da aus ihnen keine personenbezogenen Daten übermittelt werden. Anders verhält es sich hingegen zumeist mit den umfangreicheren Karteien. Sie müssen sich regelmäßig an § 9 LDSG messen lassen. Dessen Voraussetzungen liegen in der Regel nicht vor. Denn für Buchführungs-, Kassen- und ähnliche Zwecke ist die Speicherung der beschriebenen Daten nicht notwendig. Auch zur Erkennung von Mehrfachtätern halte ich das Führen einer örtlichen Bußgeldkartei nicht für zulässig. Dies ergibt sich aus Sinn und Zweck des beim Kraftfahrtbundesamt eingerichteten Verkehrszentralregisters, das eine Vielzahl örtlicher Karteien ersetzen sollte. Auch der neue Entwurf eines Verkehrszentralregistergesetzes (BT-Drs. 8/3900) geht davon aus, daß schon nach geltendem Recht die Führung sog. schwarzer Listen verboten ist, ohne allerdings diesen Begriff näher zu erläutern. Ich schlug dem Innenministerium vor, in einem Erlaß die Frage des Führens örtlicher Bußgeldkarteien in diesem Sinne zu klären und im übrigen auf eine eindeutige Regelung im künftigen Verkehrszentralregistergesetz hinzuwirken.

4.3 Führerscheinkarteien

Die unteren Verwaltungsbehörden haben über die ausgehändigten Führerscheine eine Kartei zu führen. Sie ist nach den Anfangsbuchstaben der Namen der Führerscheininhaber zu ordnen. Den Inhalt der Kartei regelt die Straßenverkehrszulassungsverordnung im übrigen nicht. Überprüfungen bei einigen Behörden ergaben, daß die Führerscheinkarteien vereinzelt noch Angaben über Verkehrsstraftaten und -übertretungen aus den fünfziger und sechziger Jahren enthalten. Ich halte dies wegen §§ 9, 13 LDSG nicht für möglich. Verkehrsstraftaten und -übertretungen dürfen nach Einrichtung des Verkehrszentralregisters nicht mehr in einer örtlichen Kartei gespeichert werden. Nach Sinn und Zweck der Führerscheinkartei dürfen dort außer den Personalien nur fahrerlaubnisrelevante Daten wie Führerscheinklasse, etwaige Auflagen, gerichtliche und verwaltungsbehördliche Fahrerlaubnisentziehungen, Fahrverbote und die Wiedererteilung der Fahrerlaubnis enthalten sein. Da die Speicherung von Ver-

kehrstraftaten nicht zulässig ist, forderte ich die Löschung dieser Daten. Das Innenministerium gab inzwischen eine solche Weisung heraus.

4.4 Karteien über eingestellte Strafverfahren nach § 153 a der Strafprozeßordnung

Aufgrund einer Kleinen Anfrage im Landtag prüfte ich, ob die unteren Verwaltungsbehörden in Führerschein- oder ähnlichen Karteien vermerken, wenn ein Ermittlungs- bzw. Strafverfahren gegen einen Bürger nach § 153 a der Strafprozeßordnung eingestellt wurde. Nach dieser Vorschrift kann mit Zustimmung des Beschuldigten von der Anklageerhebung abgesehen bzw. ein Verfahren eingestellt werden, wenn bestimmte Auflagen und Weisungen geeignet sind, bei geringer Schuld das öffentliche Interesse an der Strafverfolgung zu beseitigen.

Bei meinen Überprüfungen ergab sich folgendes:

- Seit 1975 trägt das Kraftfahrtbundesamt in das Verkehrszentralregister auch Entscheidungen der Staatsanwaltschaften und der Gerichte nach § 153 a der Strafprozeßordnung ein. Rechtsgrundlage hierfür ist der damals neu geschaffene § 13 Abs. 1 Nr. 3 a der Straßenverkehrszulassungsordnung. Diese Entscheidungen bepunktet das Kraftfahrtbundesamt im Gegensatz zu rechtskräftigen Entscheidungen der Gerichte und Verwaltungsbehörden nicht. Es teilt sie lediglich den Verwaltungsbehörden mit, wenn diese anfragen oder der Betroffene wegen anderer Verkehrsverstöße mindestens 9 Punkte erreicht hat.
- Die Verwaltungsbehörden nehmen die Mitteilung des Kraftfahrtbundesamtes jeweils zu den Führerscheinakten des einzelnen Bürgers. Diese Akten sind Grundlage ihres weiteren Vorgehens.
- Das Innenministerium vertrat von Anfang an die Auffassung, Entscheidungen nach § 153 a StPO seien in Fahrerlaubnis-Entziehungsverfahren zu berücksichtigen. Seit Anfang 1979 ließ es die Verfahrenseinstellungen generell bepunktet und der vom Kraftfahrtbundesamt mitgeteilten Punktezahl zuschlagen. Weder die Betroffenen noch Gericht oder Staatsanwaltschaft erfuhren zunächst von dieser Weisung an die Verkehrsbehörden.
- Bei den Verwaltungsbehörden stellte ich eine erhebliche Unsicherheit darüber fest, ob und wie lange derartige Entscheidungen verwertet werden dürfen.
- Keine Verwaltungsbehörde hatte in einer Kartei Entscheidungen nach § 153 a StPO vermerkt. Allerdings führt ein Landratsamt seit einigen Jahren zu statistischen Zwecken eine Liste, in die jahrgangweise unter einer fortlaufenden Nummer die Personalien derjenigen eingetragen werden, gegen die ein Verfahren nach § 153 a StPO eingestellt wurde.

Der eigentliche Kern des Problems ist nicht die Eintragung eingestellter Verfahren in einer Kartei oder Liste, sondern die Verwertung dieser Eintragungen. Ich habe erhebliche Zweifel, ob Entscheidungen von Gerichten oder Staatsanwaltschaften, denen keine rechtskräftige Schuldfeststellung zugrunde liegt, zum Nachteil des Betroffenen verwertet, insbesondere bepunktet werden dürfen. In jedem Fall halte ich jedwede Verwertung einer Verfahrenseinstellung nach Tilgung der Entscheidung im Verkehrszentralregister für unzulässig. Schwere Bedenken äußerte ich auch gegen die Punktepraxis und darüber, daß der

Betroffene über die Rechtsfolgen seiner Zustimmungserklärung zur Verfahrenseinstellung im unklaren gelassen wurde. Ich schlug ferner vor, das Führen besonderer Listen über Verfahrenseinstellungen wegen der für den Betroffenen damit verbundenen Gefahren zu untersagen. Darüber hinaus regte ich an, im künftigen Verkehrszentralregistergesetz einige bei der Überprüfung zu Tage getretene Datenschutzprobleme eindeutig zu klären.

Das Innenministerium trug meinen Vorstellungen sehr rasch weitgehend Rechnung. Es ordnete an, Entscheidungen nach § 153 a StPO nicht mehr zu bepunkten, sondern nur im Einzelfall zu würdigen. Die Verwertung getilgter Eintragungen untersagte es. Auch empfahl es den Verwaltungsbehörden, keine besonderen Listen über Entscheidungen nach § 153 a StPO zu führen.

5. Meldewesen

5.1 Allgemeines

Das Landesdatenschutzgesetz fügte in das Meldegesetz datenschutzrechtliche Bestimmungen ein, die den allgemeinen Datenschutzvorschriften vorgehen. Nach dem Meldegesetz richten sich allerdings nur die Datenübermittlungen an Polizeidienststellen durch Gewährung der Einsicht in das Melderegister (§ 15 a MG), Auskünfte an Privatpersonen und öffentliche Stellen des Auslandes (§ 15 b MG) und Veröffentlichungen von Einwohnerdaten (§ 15 c MG). Im übrigen sind die Übermittlungsvorschriften des Landesdatenschutzgesetzes anzuwenden.

Zahlreiche Anfragen von Behörden, Überprüfungen im Rahmen von Eingaben und Informations- bzw. Kontrollbesuche bei den Meldebehörden zeigten, daß die Durchsetzung und Anwendung der neuen Vorschriften erhebliche Schwierigkeiten bereitet. Ich sehe dafür verschiedene Gründe:

- Anfangs wußten viele Meldebehörden nicht, daß durch das Landesdatenschutzgesetz datenschutzrechtliche Vorschriften in das Meldegesetz eingefügt wurden. Weder Innenministerium noch Regierungspräsidien wiesen auf die neue Rechtslage hin.
- Mitunter wird die den melderechtlichen Datenschutzvorschriften zugrunde liegende Systematik (einfache und erweiterte Melderegisterauskunft, Gruppenauskunft) nicht verstanden.
- Die Auslegung unbestimmter Rechtsbegriffe („berechtigtes Interesse“, „öffentliches Interesse“) wirft Probleme auf.
- Ungünstig wirkt sich schließlich auch die (formale) Weitergeltung der zum Teil überholten Verwaltungsvorschriften des Innenministeriums zum Meldegesetz aus.

Die vielen Anfragen sind jedoch ein Beweis dafür, daß sich die meisten Meldebehörden um eine gesetzmäßige Handhabung bemühen und das Datenschutzbewußtsein der Bediensteten erfreulich entwickelt ist. Vereinzelt ist die Praxis der Meldebehörden sogar strenger als die Datenschutzvorschriften dies verlangen. Das rege Interesse der Meldebehörden ist mit Grund dafür, daß ich bereits jetzt einen zuverlässigen Überblick über die vielen Datenschutzfragen im Meldewesen habe. Einige Problembereiche werden auch für das neue Landesmeldegesetz von Bedeutung sein, mit dem sich der Landtag bald befassen wird.

5.2 Handhabung des geltenden Melderechts

5.2.1 Erhebung von Meldedaten

Die Meldebehörden erheben zum Teil mehr Daten als zulässig ist.

— Meldung des Hauptmeldepflichtigen (§ 4 MG)

Nach § 4 MG hat der Hauptmeldepflichtige für die An- und Abmeldung einen Meldeschein zu verwenden, dessen Inhalt durch Rechtsverordnung vorgeschrieben ist. Ich stellte bei meinen Kontrollen fest, daß die Meldebehörden einen Vordruck verwenden, der die Erhebung einiger zusätzlicher Daten, z. B. Tag der Eheschließung und Tag der Scheidung, vorsieht. Das Innenministerium untersagte dies inzwischen.

— Meldung des Wohnungsgebers (§ 5 MG)

Nach § 5 MG hat der Wohnungsgeber nach einem Ein- oder Auszug schriftlich die Anschrift der Wohnung, den Namen des Wohnungsinhabers und das Datum des Ein- oder Auszugs zu melden. Einige Meldebehörden fordern vom Wohnungsgeber unter Verwendung eines — von einem Verlag herausgegebenen nicht amtlich vorgeschriebenen Vordrucks — zusätzliche Angaben, z. B. Zahl der Familienangehörigen. Dies ist unzulässig. Ich bat den Verlag, sein Formular zu ändern.

5.2.2 Speicherung von Meldedaten

Personenbezogene Daten dürfen im Melderegister nur gespeichert werden, soweit sie zur rechtmäßigen Aufgabenerfüllung der Gemeinden erforderlich sind. Dies wird von den Meldebehörden bisher kaum beachtet. Es ist derzeit auch schwierig zu beurteilen, welche Daten zur Aufgabenerfüllung benötigt werden. Nr. 34 der Verwaltungsvorschriften des Innenministeriums zum Meldegesetz zählt zwar die Daten auf, die im Melderegister „mindestens“ gespeichert sein müssen. Diese Bestimmung kann nach Inkrafttreten des Landesdatenschutzgesetzes nur noch ein Anhaltspunkt für die Erforderlichkeit der Speicherung eines einzelnen Datums sein. Auch § 2 des Melderechtsrahmengesetzes, der den Inhalt des Melderegisters allerdings nicht abschließend festlegt, ist nur eine Orientierungshilfe, da ihm keine unmittelbare Geltung zukommt. Umstritten ist derzeit beispielsweise, ob die Zugehörigkeit zu einer nicht öffentlich-rechtlichen Religionsgesellschaft im Melderegister gespeichert werden darf. Ich bezweifle dies und bin dabei, diese und einige weitere Fragen mit dem Innenministerium zu klären.

5.2.3 Übermittlung von Meldedaten

a) Auskunft an Stellen außerhalb des öffentlichen Bereichs

— Anwendungsbereich des § 15 b MG

§ 15 b MG regelt nur die Erteilung von Auskünften aus dem Melderegister an Stellen außerhalb des öffentlichen Bereichs. Welche Stellen zum öffentlichen Bereich gehören und damit von der Regelung des § 15 b MG nicht betroffen sind, ergibt sich aus der Verweisung auf § 10 und § 21 LDSG. Nicht ausdrücklich erwähnt werden in diesen Vorschriften

die Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung (§ 20 LDSG). Da es sich bei diesen jedoch ebenfalls um öffentliche Stellen im Sinne des § 10 Abs. 1 LDSG handelt, § 20 LDSG lediglich eine Ausnahme von § 10 LDSG darstellt und nichts für eine Sonderbehandlung dieser Stellen gegenüber dem sonstigen öffentlichen Bereich spricht, werden sie von § 15 b MG nicht erfaßt. Dies übersehen die Meldebehörden immer wieder.

— Einfache Melderegisterauskunft (§ 15 b Abs. 2 MG)

Nach § 15 b Abs. 2 MG darf die Meldebehörde Auskunft über Namen und Anschriften einer oder mehrerer namentlich bezeichneter Personen erteilen.

Die Meldebehörden fragen immer wieder, ob sie eine Auskunft auch dann erteilen dürfen, wenn eine Person inzwischen weggezogen ist. Dies ist zu bejahen. Allerdings wird die Wegzugsmeldebehörde im Interesse des Betroffenen von Amts wegen prüfen müssen, ob bei der Zuzugsmeldebehörde eine Auskunftssperre (§ 15 b Abs. 7 MG) besteht. Der Betroffene wird regelmäßig nicht damit rechnen, daß die „frühere“ Meldebehörde noch Auskünfte aus dem Melderegister erteilt. Eine eindeutige Regelung im neuen Landesmeldegesetz erscheint erforderlich.

— Erweiterte Melderegisterauskunft (§ 15 b Abs. 3 MG)

• Telefonische Auskunft

Von erheblicher praktischer Bedeutung ist die Frage, ob erweiterte Melderegisterauskünfte telefonisch erteilt werden dürfen. Ich möchte dies nicht generell verneinen, die Meldebehörden aber zugleich zu größter Sorgfalt ermuntern. Sie dürfen nur an Berechtigte Daten übermitteln. Dabei müssen sie ihren Gesprächspartner eindeutig identifizieren können. Hinzu kommt, daß dieser für die Datenübermittlung nach § 15 b Abs. 3 MG ein berechtigtes Interesse nachweisen muß. Der Nachweis wird häufig nur durch schriftliche Unterlagen zu erbringen sein.

• Auskunft an Kreditschutzorganisationen

Wiederholt wurde ich gefragt, unter welchen Voraussetzungen die Meldebehörden an Kreditschutzorganisationen Auskünfte erteilen dürfen. Ich meine, daß auch wirtschaftliche Interessen berechnete Interessen im Sinne des § 15 b Abs. 3 MG sein können. Ein berechtigtes Interesse wird allerdings fehlen, wenn der Antragsteller es unterließ, sich die Daten in zumutbarer Weise selbst zu beschaffen. Kreditgeber können die Daten häufig bei ihren Vertragspartnern offen erheben. Auch können sie den Vertragspartner um Vorlage einer Meldebestätigung bitten. Das berechnete Interesse muß im Einzelfall für jedes einzelne Datum nachgewiesen werden, über das Auskunft begehrt wird. Pauschale Begründungen, wie z. B. „zur Prüfung der Kreditwürdigkeit“, genügen dabei nicht.

— Gruppenauskunft (§ 15 b Abs. 4 MG)

• Auskunft an politische Parteien zu Wahlzwecken

Da während der letzten Monate Landtags-, Kommunal- und Bundestagswahlen stattfanden, erkundigten sich zahlreiche Bürger und Behörden wie auch die Presse danach, ob die Meldebehörden politischen Parteien im Zusammenhang mit ihrer Beteiligung an Wahlen Auskünfte über bestimmte Wählergruppen (z. B. Jung- oder Altwähler) erteilen dürfen. Ich bejahte dies mit der Begründung, im Hinblick auf die verfassungsrechtlich gewährleistete Mitwirkung der Parteien bei der politischen Willensbildung bestehe ein öffentliches Interesse an der Auskunftserteilung. Es dürfen allerdings nur bestimmte Daten mitgeteilt und andere abschließend aufgeführte Daten der Auswertung zugrunde gelegt werden. So darf beispielsweise die Meldebehörde nicht das Geburtsdatum oder das Geburtsjahr, sondern lediglich die Zugehörigkeit zu bestimmten Altersgruppen mitteilen. Auch kann sie die Auskunft nur innerhalb eines Zeitraums von sechs Monaten vor einer Wahl und nur für Wahlzwecke geben. Die Meldebehörden können dem Datenempfänger außerdem Datensicherungsmaßnahmen vorschreiben.

• Auskunft an Kandidaten bei Bürgermeisterwahlen

Eine Meldebehörde teilte im Zusammenhang mit einer Bürgermeisterwahl zwei von politischen Parteien unterstützten Bewerbern bestimmte Daten über Altwähler mit. Ich beanstandete dies, da an der Auskunftserteilung kein öffentliches Interesse besteht. Bei Bürgermeisterwahlen steht nach dem Kommunalwahlrecht das persönliche Interesse des Bewerbers an seiner Wahl im Vordergrund. Politische Parteien können sich nicht selbst an der Wahl beteiligen, so daß sich das öffentliche Interesse hier nicht mit ihrer besonderen verfassungsrechtlichen Stellung begründen läßt.

• Auskunft an Banken, Versicherungen usw.

Die Meldebehörden dürfen Banken, Sparkassen und Versicherungen keine Auskünfte mehr zu Werbezwecken erteilen, da das Interesse der Wirtschaft an Adressenmaterial kein öffentliches Interesse begründet. Die anfänglich weitergehende Praxis vieler Meldebehörden beobachtete ich in letzter Zeit nicht mehr.

— Veröffentlichung von Jubiläumsdaten (§ 15 c Abs. 1 MG)

Die Meldebehörden dürfen nach § 15 c MG bestimmte Jubiläumsdaten veröffentlichen, wenn der Betroffene der Veröffentlichung nicht widerspricht. Bei Kontrollbesuchen stellte ich fest, daß Meldebehörden zum Teil über diese Regelung hinausgehen und personenbezogene Daten nur mit Einwilligung der Betroffenen veröffentlichen. Überrascht hat mich, daß sogar in kleinen Gemeinden nicht wenige Bürger der Veröffentlichung widersprechen.

Vereinzelt besteht das Mißverständnis, die Meldebehörden müßten Jubiläumsdaten auf jeden Fall an die Presse weitergeben, da diese einen Informationsanspruch habe.

— Veröffentlichung von Einwohnerdaten in Einwohnerbüchern (§ 15 c Abs. 2 MG)

Nach § 15 c Abs. 2 MG können bestimmte Einwohnerdaten in Einwohnerbüchern und ähnlichen Nachschlagewerken veröffentlicht werden. In der Praxis wird mitunter übersehen, daß danach auch die Mitteilung bestimmter Auswahlkriterien wie „Haushaltungsvorstand“ oder „erwerbstätige Ehefrauen“ nicht mehr zulässig ist. Gleiches gilt für das Datum „Hauseigentümer“, sofern es dem Melderegister entnommen wird. Ist es in der Grundsteuerdatei gespeichert, unterliegt es dem Steuergeheimnis.

Vereinzelt — vor allem im südbadischen Raum — werden auch noch sogenannte Ortssippenbücher herausgegeben, in denen eine Vielzahl von Einwohnerdaten enthalten sind. Ich wies wiederholt darauf hin, daß auch Ortssippenbücher der Regelung des § 15 c MG unterfallen, soweit die Daten dem Melderegister entnommen werden. Handelt es sich um Daten der Personenstandsbücher, so dürfte § 61 des Personenstandsgesetzes einer Veröffentlichung entgegenstehen.

— Widerspruchsrecht des Einwohners gegen die Veröffentlichung (§ 15 c Abs. 3 MG)

§ 15 c Abs. 3 MG verpflichtet die Gemeinden, Einwohner durch öffentliche Bekanntmachung auf ihr Widerspruchsrecht hinzuweisen. Die Belehrung ist nach meinen bisherigen Beobachtungen nicht immer zutreffend, beispielsweise wird für die Einlegung des Widerspruchs zu Unrecht Schriftform verlangt.

b) Übermittlung von Meldedaten an Polizeidienststellen durch Einsichtnahme in das Melderegister (§ 15 a MG)

Polizeidienststellen sind befugt, zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben jederzeit in das Melderegister Einsicht zu nehmen. Die Polizei vertrat vielerorts die Auffassung, daß der Ausdruck personenbezogener Daten durch die regionalen Rechenzentren durch diese Vorschrift gedeckt ist. Dies trifft nicht zu, da unter „Melderegister“ nur die herkömmliche, alphabetisch geordnete Datei, nicht jedoch die automatisierte Einwohnerdatei zu verstehen ist. Dies ergibt sich aus der Allgemeinen Verwaltungsvorschrift zum Meldgesetz. § 15 a gewährt daher kein unmittelbares Zugriffsrecht auf automatisierte Dateien. Es wurde überdies verkannt, daß § 15 a lediglich die Datenübermittlung in Form der Einsichtnahme, nicht jedoch die Datenweitergabe regelt.

Schwierigkeiten bereitet gelegentlich auch die Frage, was die Meldebehörde im Rahmen des § 15 a MG zu prüfen hat. Nach meiner Auffassung trägt hier, anders als im Rahmen des § 10 LDSG, allein die Polizeidienststelle die Verantwortung für das Vorliegen der materiellen Voraussetzungen. Die Meldebehörde muß sich

lediglich vergewissern, daß es sich um einen einer einsichtsberechtigten Polizeidienststelle angehörenden Polizeibeamten handelt.

c) Weitergabe von Meldedaten an Behörden und sonstige öffentliche Stellen (§ 10 LDSG)

— Prüfungspflicht der Meldebehörden

Die Meldebehörden haben im Rahmen des § 10 LDSG zu prüfen, ob die anfordernde Behörde die verlangten Daten ihrer Art und ihres Umfangs nach generell zur Erfüllung ihrer Aufgaben benötigt. Dies wird von den Meldebehörden häufig übersehen; sie übermitteln Daten aus dem Melderegister, ohne sich von der anfordernden Behörde die Erforderlichkeit der Datenübermittlung darlegen zu lassen.

— Zur Aushändigung von Einwohnerlisten an die Polizei

Einige Polizeidienststellen baten Meldebehörden, ihnen einmal jährlich eine Liste aller Einwohner zur Verfügung zu stellen. Dies sollte der Polizei die Einholung von Einzelauskünften oder die Einsichtnahme in das Melderegister ersparen. Ich halte ein solches Vorgehen nicht für zulässig; die Datenübermittlung ist nicht erforderlich; auch habe ich Zweifel an der Geeignetheit einer solchen Maßnahme geäußert. Das Innenministerium teilt meine Auffassung und unterrichtete die Polizeidienststellen hiervon.

— Weitergabe von Meldedaten an die Polizei durch regionale Rechenzentren

Nach § 13 des Gesetzes über die Datenzentrale dürfen die regionalen Rechenzentren über die EDV-Datenbestände des automatisiert geführten Einwohnerwesens nur mit Zustimmung der Gemeinden verfügen. Einige Polizeidienststellen ersuchten die Gemeinden ihres Zuständigkeitsbereichs, ihr regionales Rechenzentrum generell zur Übermittlung von Daten an die Polizei zu ermächtigen. Ich halte dies nicht für zulässig, weil auch Polizeidienststellen im Rahmen des § 10 LDSG ihre Auskunftersuchen begründen müssen und auch das Vorliegen der gesetzlichen Voraussetzungen für eine Datenübermittlung geprüft werden muß. Die Prüfung muß der Herr der Daten, also die Gemeinde, vornehmen, da sie auch die Verantwortung trägt und ihrer Kontrollfunktion gegenüber dem Rechenzentrum gerecht werden muß. Zulässig wäre allerdings, daß die Gemeinde ihre Zustimmung im voraus für genau umschriebene Fallgruppen erteilt, bei denen die Datenübermittlung stets zulässig ist. Mir erscheint jedoch fraglich, ob sich derartige Fallgruppen bilden lassen. Nicht genügen kann z. B., die regionalen Rechenzentren zur Auskunftserteilung „für Zwecke der Strafverfolgung“ zu ermächtigen. Unter dem Gesichtspunkt der Erforderlichkeit und der Verhältnismäßigkeit kommt es nämlich auf die Art der Straftat und die Tatumsstände an.

- Datenübermittlungen an Behörden und sonstige öffentliche Stellen in Form der Weitergabe von Meldescheinen bzw. -bestätigungen (§§ 10, 29 LDSG)

Das Landesdatenschutzgesetz bestimmt, daß sein § 10 erst ab 1. Januar 1983 anzuwenden ist, soweit Meldebehörden im Zeitpunkt des Inkrafttretens des LDSG an Behörden und sonstige öffentliche Stellen personenbezogene Daten durch Weitergabe der „Meldescheine“ übermitteln. Nr. 21 der Verwaltungsvorschriften des Innenministeriums zum Meldegesetz sieht andererseits vor, daß die Meldebehörden den Polizeidienststellen eine Durchschrift jeder „Meldebestätigung“ übermitteln. Ich halte diese Datenübermittlung nach Sinn und Zweck des § 29 LDSG weiterhin für zulässig, zumal die Meldebestätigung weniger Daten enthält als die Meldescheine. Unzulässig ist dagegen die teilweise zu beobachtende Praxis, den Polizeidienststellen Meldescheine zu überlassen.

- Behördeninterne Weitergabe der Meldescheine

Häufig geben die Einwohnermeldeämter innerhalb des Bürgermeisteramtes an andere Ämter Durchschriften der Meldescheine weiter. Dieses Verfahren wird weder von § 10 noch von § 29 LDSG erfaßt, da es sich hierbei nicht um eine Datenübermittlung an eine andere Behörde handelt. Nach § 7 LDSG darf jedoch auch innerhalb einer Behörde jeder Beschäftigte nur die personenbezogenen Daten erhalten, die er zur Wahrnehmung seiner Aufgaben benötigt. Zumeist benötigen die Ämter nur einzelne Angaben aus den Meldescheinen, nicht dessen ganzen Inhalt. Ich legte deshalb einigen Gemeinden eine Änderung ihrer Praxis nahe, wegen der in § 29 LDSG festgelegten Übergangsfrist forderte ich jedoch nicht eine sofortige Umstellung.

- d) Datenübermittlung der Meldebehörden an den Bundesgrenzschutz für Zwecke der Personalwerbung

Die Meldebehörden haben auch die Wehrpflichtigen zu erfassen. Der Bundesgrenzschutz ist an der Weitergabe der dabei gewonnenen Personaldaten für Zwecke der Nachwuchswerbung interessiert. Ich vertrat gegenüber dem Innenministerium die Auffassung, daß eine Datenübermittlung in diesen Fällen nach § 10 LDSG unzulässig ist, da die Kenntnis der Daten für den Datenempfänger nicht erforderlich, sondern allenfalls zweckmäßig ist. Entgegen der Ansicht des Bundesministers des Innern und des Bundesbeauftragten für den Datenschutz kann die Nachwuchswerbung auch in anderer Form wirksam betrieben werden, insbesondere in Form von Zeitungsinserten oder Informationsveranstaltungen vor Ort. Durch die Datenübermittlung wird auch nicht — wie der Bund meint — eine aufwendige und zu Lasten des Bundes gehende Doppelerhebung (Bundeswehr, Bundesgrenzschutz) vermieden, da der Bundesgrenzschutz Namen und Anschrift der Wehrpflichtigen nicht aufgrund einer Rechtsvorschrift erheben kann. Eine Offenbarungspflicht der Wehrpflichtigen besteht lediglich nach dem Wehrpflichtgesetz, nicht nach dem Bundesgrenzschutzgesetz. Der Wehrpflichtige würde überdies bei der Wehrrfassung über die Bedeutung seiner Erklärung

getäuscht, wenn seine Angaben entgegen der Belehrung in dem von ihm auszufüllenden Vordruck an den Bundesgrenzschutz weitergeleitet würden. Auch § 49 des Bundesgrenzschutzgesetzes rechtfertigt die Datenübermittlung nicht, da Wehrpflichtige derzeit nicht zwangsweise zum Grenzschutzdienst eingezogen werden.

5.2.4 Erteilung von Auskünften an Einwohner (§ 15b Abs. 1 MG)

Die Meldebehörde muß jedem Einwohner auf Antrag Auskunft erteilen über die zu seiner Person gespeicherten Daten und über die Empfänger erweiterter Melderegisterauskünfte der letzten zwei Jahre. Um dieser Verpflichtung genügen zu können, muß die Meldebehörde derartige Datenübermittlungen in geeigneter Weise festhalten, z. B. durch Protokollierung auf der Melderegisterkarte, Vermerk in sonstigen ohne weiteres zugänglichen Unterlagen, Aufbewahren von Auskunftersuchen. Dies wird vielfach nicht beachtet. Unklar ist mitunter auch, welche Datenübermittlungen festgehalten werden müssen. Aus dem Wortlaut und der Entstehungsgeschichte ergibt sich, daß einfache Melderegisterauskünfte, Gruppenauskünfte und Datenübermittlungen nach §§ 10, 20, 21 LDSG dem Betroffenen nicht mitzuteilen und folglich auch nicht zu „protokollieren“ sind.

5.2.5 Sperrung und Löschung von Meldedaten

Eine Sperrung und Löschung von zur rechtmäßigen Aufgabenerfüllung nicht mehr benötigter Meldedaten findet gegenwärtig nicht statt. Ich konnte lediglich feststellen, daß die Karteikarten weggezogener oder verstorbener Bürger vom Hauptregister in ein Nebenregister überführt werden. Dies ist jedoch keine Sperrung im Sinne des Landesdatenschutzgesetzes, da die Daten nach wie vor übermittelt oder sonst genutzt werden. Das Innenministerium sollte den Meldebehörden Hinweise zur Handhabung des § 13 LDSG geben, die sich bereits an dem im Lande noch umzusetzenden § 10 des Melderechtsrahmengesetzes orientieren.

5.2.6 Datensicherungsmaßnahmen

Nach den Verwaltungsvorschriften zum Meldegesetz muß die Zuzugsmeldebehörde der Wegzugsmeldebehörde die Anmeldung unter Verwendung eines Vordrucks mitteilen, der einige personenbezogene Daten enthält. Der Vordruck wird üblicherweise offen versandt. Ich äußerte im Hinblick auf § 8 LDSG hiergegen Bedenken. Das Post- und Amtsgeheimnis schützt nicht vor einer Kenntnisnahme der Daten, sondern nur vor einer unbefugten Weitergabe. Das Innenministerium empfahl auf meine Anregung hin den Meldebehörden inzwischen, die Rückmeldung im verschlossenen Umschlag zu versenden.

5.3 Melderechtsrahmengesetz und künftiges Landesmeldegesetz

5.3.1 Melderechtsrahmengesetz

Der Bund hat aufgrund seiner Rahmengesetzgebungskompetenz für das Meldewesen (Artikel 75 Nr. 5 GG) ein Melderechtsrahmengesetz erlassen. Es enthält keine für die Meldebehörden unmittelbar geltenden Vorschriften. Die Länder sind nach § 23 MRRG verpflichtet, ihr Melderecht bis August 1982 dem MRRG anzupassen.

Das Gesetz steht unter dem Primat des Datenschutzes. Es verfolgt vor allem den Zweck, einen wirksamen bereichsspezifischen Datenschutz im Meldewesen zu gewährleisten. Die jetzige Regelung unterscheidet sich damit wesentlich von früheren Gesetzentwürfen der Bundesregierung, die eine möglichst große Verwaltungseffizienz und einen ungehinderten Datenfluß zwischen den Meldebehörden und allen anderen Behörden zum Ziel hatten. Das Melderechtsrahmengesetz enthält gegenüber dem geltenden Melde- und Datenschutzrecht in datenschutzrechtlicher Hinsicht folgende Abweichungen:

- Die im Melderegister zulässigerweise zu speichernden Daten werden katalogmäßig aufgezählt; der Katalog kann allerdings durch Landesgesetz erweitert werden. Nach dem MRRG wird die Berufsangabe nicht mehr gespeichert.
- Die im Melderegister gespeicherten Daten unterliegen einer Zweckbindung.
- Die zur Aufgabenerfüllung nicht mehr erforderlichen Daten sind nicht nur zu sperren, sondern zu löschen. Dies gilt insbesondere — allerdings mit gewissen Einschränkungen — für die Daten eines weggezogenen oder verstorbenen Einwohners.
- Für die Übermittlung bestimmter sensitiver Daten an andere Behörden gelten strengere Voraussetzungen als gegenwärtig in § 10 Abs. 1 LDSG.
- Für die Übermittlung bestimmter sensitiver Daten an Sicherheitsbehörden gelten besondere Vorschriften. Die Prüfung der Übermittlungsvoraussetzungen durch die Meldebehörden wird teilweise entfallen. Statt dessen werden die Sicherheitsbehörden verpflichtet, Aufzeichnungen über die auf ihre Veranlassung von den Meldebehörden durchgeführten Datenübermittlungen zu führen, um eine Nachprüfung durch den Datenschutzbeauftragten zu ermöglichen.
- Regelmäßige Datenübermittlungen an andere Behörden sind künftig nur zulässig, wenn dies in einer Rechtsnorm bestimmt ist.
- Für den Datenaustausch innerhalb eines Bürgermeisteramts gelten die Datenübermittlungsvorschriften entsprechend.
- Die Datenübermittlungen an Religionsgesellschaften werden auf eine klare gesetzliche Grundlage gestellt.
- Für die Erteilung einer erweiterten Melderegisterauskunft genügt künftig die Glaubhaftmachung des berechtigten Interesses statt des Nachweises. Allerdings ist der Betroffene über die Erteilung einer Auskunft nachträglich zu unterrichten.

5.3.2 Landesmeldegesetz

Bei der Umsetzung des Melderechtsrahmengesetzes in ein neues Landesmeldegesetz muß die datenschutzfreundliche Grundkonzeption erhalten bleiben.

- Vor allem werde ich darauf achten, daß der Datenkatalog des § 2 Abs. 1 und 2 MRRG nicht ohne zwingenden Grund erweitert wird. Ich bin sogar der Auffassung, daß nicht alle der im MRRG genannten Angaben im Melde-

- register gespeichert werden müssen. Bei einzelnen Daten, die nur statistischen Zwecken dienen, genügt die Erhebung und Weitergabe an das Statistische Landesamt.
- Verhindert werden muß auch, daß der in § 12 Abs. 1 MRRG erstmals festgelegte objektive Begriff der „Hauptwohnung“ eines Einwohners zu intensiven Nachforschungen der Meldebehörden bei der Anmeldung des Einwohners führt.
 - Die Regelung über die Datenübermittlungen an andere Behörden und sonstige öffentliche Stellen (§ 18 MRRG) bedarf teilweise der Präzisierung, insbesondere müssen die Prüfungspflichten der Meldebehörden verdeutlicht werden.
 - Für überlegenswert halte ich auch, ob die nach dem geltenden Melderecht (§ 15 b Abs. 1 MG) nur für erweiterte Melderegisterauskünfte bestehende Protokollierungspflicht nicht auch für bestimmte Datenübermittlungen an andere Behörden eingeführt werden sollte.
 - Soweit § 19 Abs. 2 Satz 2 MRRG dem Landesgesetzgeber die Möglichkeit eröffnet, öffentlich-rechtlichen Religionsgesellschaften weitere Daten von Nichtmitgliedern zu übermitteln, sollte Zurückhaltung geübt werden. Nach § 19 Abs. 3 MRRG setzt eine Datenübermittlung an die öffentlich-rechtlichen Religionsgesellschaften voraus, daß diese ausreichende Datenschutzmaßnahmen getroffen haben. Diese Regelung entspricht § 21 LDSG. Die einzelnen Meldebehörden können das Vorliegen dieser Voraussetzungen nicht nachprüfen, da nicht auf das Bestehen kirchlicher Datenschutzgesetze, sondern auf die tatsächlich getroffenen Datensicherungsmaßnahmen abzustellen ist. Es gilt deshalb, im neuen Landesmeldegesetz hierfür ein befriedigendes Verfahren zu finden.
 - Die Regelung über die Erteilung erweiterter Melderegisterauskünfte (§ 21 Abs. 2 MRRG) wird nochmals daraufhin zu prüfen sein, ob nicht eine vorherige statt einer nachträglichen Unterrichtung des Betroffenen zulässig und zweckmäßig ist. Die derzeit geltende Bestimmung über die Erteilung von Gruppenauskünften sollte im wesentlichen übernommen werden, wobei allerdings die Regelung über die zulässigen Auswahlkriterien aufgrund praktischer Erfahrungen verdeutlicht werden müßte.
 - § 24 MRRG gestattet bis 31. Dezember 1985 Übergangsregelungen für die Einsichtnahme der Polizei in das Melderegister. Möglicherweise kann diese Frist abgekürzt werden.

6. Paßwesen

Wegen der geplanten Einführung neuer Personalausweise zum 1. Oktober 1981 wurden durch Gesetz vom 6. März 1980 (BGBl. I S. 270) einige datenschutzrechtliche Regelungen in das Personalausweisgesetz aufgenommen. Künftig soll die Bundesdruckerei die Personalausweise herstellen. Dabei darf sie nach § 3 Abs. 3 des Personalausweisgesetzes nur alle Seriennummern ausschließlich zum Nachweis des Verbleibs der Ausweise speichern. Die Speicherung weiterer Daten ist unzulässig.

Ursprünglich plante der Bund ein Herstellungsverfahren, bei dem die Bundesdruckerei die Personalausweisdaten bis zu drei Tagen hätte speichern müssen. Ein solches Verfahren verstößt gegen § 3 Abs. 3 des Bundespersonalausweisgesetzes. Der Plan des Bundes stieß daher bei allen Datenschutzbeauftragten auf erheblichen Widerstand.

Der Bundesminister des Innern stellte sodann ein neues Verfahren vor. Es unterscheidet sich vom ursprünglichen darin, daß die Ausweisdaten bei elektronischer Erfassung bereits nach wenigen Sekunden, bei manueller Eingabe nach wenigen Minuten gelöscht werden können. Das neue Verfahren ist aus der Sicht des Datenschutzes zwar eine Verbesserung. Aber es verstößt ebenso gegen § 3 Abs. 3 des Bundespersonalausweisgesetzes, da nach wie vor personenbezogene Daten gespeichert werden. Denn auch für das Personalausweisgesetz gilt mangels abweichender Regelungen die Legaldefinition von „Speicherung“ durch die Datenschutzgesetze. Sie verstehen hierunter das „Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung“. Genauso liegen die Dinge auch hier. Die Ausweisdaten würden nämlich auf einem Datenträger erfaßt und ihre weitere Verwendung wäre nicht lediglich auf maschineninterne Vorgänge beschränkt.

Trotz der fortgeschrittenen Zeit müssen alle Beteiligten auch weiterhin nach einer Lösung suchen. Bislang können leider auch die Datenschutzbeauftragten kein Verfahren anbieten, das mit dem geltenden Recht in Einklang steht, den Sicherheitsanforderungen an die neuen Personalausweise genügt und praktikabel ist.

2. Abschnitt: Gesundheits- und Sozialwesen

1. Gesundheitswesen

1.1 Gesundheitsämter

Die Gesundheitsämter haben wichtige Aufgaben auf dem Gebiet der Gesundheitsvorsorge, der gesundheitlichen Überwachung und der Gesundheitshilfe. Diese umfassende Aufgabenstellung bringt es mit sich, daß sie Angaben über die gesundheitlichen und sozialen Verhältnisse vieler Einwohner ihres Bezirks sammeln. Um mir einen Einblick in die dabei entstehenden datenschutzrechtlichen Probleme zu verschaffen, unterzog ich vier staatliche Gesundheitsämter in verschiedenen Regierungsbezirken einer Überprüfung.

1.1.1 Vordrucke

Die Gesundheitsämter verwenden in großer Zahl unterschiedlich ausgestaltete, teilweise veraltete Erhebungs- und Untersuchungsbogen, Karteikarten u. ä. Diese Vordrucke sind noch nicht an die durch das Landesdatenschutzgesetz geschaffene Rechtslage angepaßt. Durch die Verwendung dieser Vordrucke besteht die Gefahr, daß

- unnötig Daten erhoben und gespeichert werden,
- der Hinweispflicht nach § 9 Abs. 2 LDSG nicht Rechnung getragen wird.

Ich halte die Einführung einheitlicher, mit den datenschutzrechtlichen Bestimmungen in Einklang stehender Vordrucke bei den Gesundheitsämtern für erforderlich. Viele Gesundheitsämter begrüßen diesen Vorschlag; die Überprüfung durch das Sozialministerium ist noch nicht abgeschlossen.

1.1.2 Aufbewahrung von Karteikarten und Akten

Nach meinen Feststellungen werden häufig nicht mehr benötigte Karteien, Karteikarten, Untersuchungsbogen sowie Einzelakten noch sehr lange Zeit aufbewahrt und erst dann vernichtet, wenn die räumlichen Verhältnisse dazu zwingen. Eine Sperrung im Sinne des § 13 Abs. 2 LDSG erfolgt noch nicht. Damit besteht die Gefahr, daß in großem Umfang nicht mehr benötigte Daten gespeichert oder in Akten gesammelt bleiben, obwohl gerade bei sensiblen Daten besonders darauf geachtet werden sollte, daß der Umfang der gespeicherten und gesammelten Daten so gering wie möglich gehalten wird. Aus diesem Grunde teilte ich dem Sozialministerium mit, daß ich aus datenschutzrechtlicher Sicht bei den Gesundheitsämtern die Schaffung genereller Aussonderungsfristen für geboten halte.

1.1.3 Dateien

Die Gesundheitsämter verarbeiten ihre Daten noch weitgehend manuell. Dabei überwiegt die aktenmäßige Behandlung. Das heißt: Befunde, Gutachten und sonstige Stellungnahmen nehmen sie in der Regel zusammen mit dem anfallenden Schriftverkehr in Akten. Parallel zu den Aktensammlungen führen sie meist Karteien, die ihnen als Hilfsmittel zum Aufsuchen der Akten und zur Kontrolle der Erledigung von Vorgängen dienen. Beschränkt sich die Funktion einer Kartei auf diese Aufgabe, handelt es sich um eine interne Datei. Auf derartige Dateien ist lediglich § 8 LDSG anzuwenden, nicht aber die übrigen Bestimmungen des Landesdatenschutzgesetzes. Vielfach sind jedoch Zweifel am internen Charakter einer Kartei angebracht und zwar dann, wenn in die Datei Krankheitsbefunde u. ä. eingetragen werden. Solcher Eintragungen bedarf es nicht, um mit Hilfe der Kartei die Akten zu erschließen. Beim Eintrag von Krankheitsbefunden spricht eine erhebliche Wahrscheinlichkeit dafür, daß dadurch das Aufsuchen der Akten erspart werden und das Karteiblatt insoweit gleichrangig neben die Akte treten soll. Dies hätte aber in den meisten Fällen zur Folge, daß man nicht mehr von einer lediglich internen Datei sprechen kann. Will man diese Rechtsfolge vermeiden, ist es erforderlich, in die Karteien keine positiven Befunde einzutragen und sie nur als Aktennachweisdatei zu führen. Negative Befunde sollten allenfalls dann eingetragen werden, wenn sich dadurch das Anliegen einzelner Akten erübrigt.

1.1.4 Schulgesundheitspflege

Die im Rahmen der Schulgesundheitspflege verwendeten Befundbogen weichen im Umfang erheblich voneinander ab. Das bedeutet, daß die einzelnen Gesundheitsämter in sehr unterschiedlichem Maße Gesundheitsdaten bei den Schülern erheben und in einer Kartei speichern. Weiter erfolgt bis jetzt noch kein Hinweis auf die Rechtsgrundlage, aus der sich die Verpflichtung zur Teilnahme an der Schuluntersuchung ergibt. In einem Teil der von mir geprüften Gesundheitsämter wird die Sammlung der Befundbögen an der Schule aufbewahrt. Ich sehe darin eine nach § 10 LDSG unzulässige Datenübermittlung und forderte deshalb die betroffenen Gesundheitsämter auf, diese Praxis aufzugeben. Bedenklich halte ich auch, daß in den meisten Fällen das Gesundheitsamt die Eltern über einen positiven

Befund durch einen offenen Handzettel informiert, der den Schülern in die Hand gedrückt wird. Bei einer derartigen Verfahrensweise besteht die große Gefahr, daß Unbefugte Kenntnis vom ärztlichen Befund erhalten. Wegen dieser Mängel legte ich dem Sozialministerium nahe, das Verfahren der Schüleruntersuchung im Rahmen der Schulgesundheitspflege und die dabei zu beachtenden datenschutzrechtlichen Vorkehrungen für alle Gesundheitsämter einheitlich zu bestimmen. Das Sozialministerium nahm dazu noch nicht abschließend Stellung.

1.1.5 Sammlung der Durchschriften ausgestellter Bescheinigungen über die soziale Beratung Schwangerer nach § 218 b Abs. 1 Nr. 1 StGB

Voraussetzung für die Straflosigkeit eines Schwangerschaftsabbruchs ist nach § 218 b Abs. 1 Nr. 1 StGB, daß eine anerkannte Beratungsstelle die Schwangere über die öffentlichen und privaten Hilfen für Schwangere, Mütter und Kinder zuvor beraten hat. Die Gesundheitsämter sind aufgrund einer Anordnung des Sozialministeriums von 1976 befugt, solche Beratungen vorzunehmen. Im Rahmen meiner Überprüfungen vor Ort stellte ich fest, daß einige der kontrollierten Ämter Sammlungen von Durchschriften der Bescheinigungen führen, die sie Schwangeren über die erfolgte soziale Beratung ausstellen. Diese Bescheinigungen enthalten Name, Geburtstag und Anschrift der Schwangeren sowie das Datum ihrer Beratung. Eines der kontrollierten Ämter heftet zudem den Durchschriften der Bescheinigungen jeweils eine Aktennotiz über die Gründe für den beabsichtigten Schwangerschaftsabbruch und die sozialen Verhältnisse der Schwangeren an. In keinem Fall holen die Gesundheitsämter die Einwilligung der Schwangeren zum Aufbewahren der Durchschrift der Bescheinigung über die Beratung und ggf. der zusätzlichen Notizen ein.

Das Sozialministerium ordnete das Führen solcher Sammlungen nicht generell an. Es wies die Gesundheitsämter lediglich durch Erlaß vom 28. Juni 1976 an, der Schwangeren auf deren Verlangen Bescheinigungen nach einem bestimmten Muster auszustellen. Darüber hinaus verpflichtete das Regierungspräsidium Stuttgart durch Erlaß vom 26. Juli 1976 die Gesundheitsämter seines Bezirks, solche Sammlungen der Durchschriften der Bescheinigungen zu führen und die einzelnen Durchschriften nach 3 Jahren zu vernichten. Das Sozialministerium teilte mir auf meine Anfrage zur Notwendigkeit dieser Sammlungen folgendes mit: Im ärztlichen Schrifttum sowie in Empfehlungen von ärztlichen Berufsverbänden werde den Ärzten zur Vermeidung des Risikos strafrechtlicher Verfolgung angeraten, auf der Vorlage, teilweise sogar der Übergabe von Beratungsbescheinigungen zu bestehen. Schwangere müßten daher damit rechnen, daß der Arzt die Durchführung des Schwangerschaftsabbruchs ablehnt, solange ihm eine soziale Beratung nicht schriftlich nachgewiesen werde. Für den Fall, daß die Schwangere eine Urschrift der Bescheinigung verliert oder der ursprünglich für eine Durchführung des Schwangerschaftsabbruchs vorgesehene Arzt den Abbruch nicht durchführt und eine Übersendung der Bescheinigung an den nunmehr für die Durchführung des Abbruchs vorgesehenen Arzt kurzfristig nicht mehr möglich ist, sollten die Gesundheitsämter jederzeit zur Ausstellung

einer Zweitschrift in der Lage sein. Dies sei den Gesundheitsämtern kurzfristig nur möglich, wenn sie zugleich mit der Urschrift eine Durchschrift herstellen und diese aufbewahren. Die von mir überprüften Gesundheitsämter trugen als weiteres Argument vor, die Sammlung sei für den Fall angelegt, daß die Bedienstete des Gesundheitsamtes, die die Beratung vornimmt, in einem Prozeß als Zeugin auftreten müsse.

Gegen die Sammlung der Durchschriften der Beratungsbescheinigungen bestehen aus der Sicht des Datenschutzes erhebliche Bedenken. Die Schwangere hat ein beachtliches, vom Gesetzgeber in verschiedenen Bestimmungen ausdrücklich als berechtigt anerkanntes Interesse an der Geheimhaltung ihrer Beratung. Jede von ihr nicht gewollte schriftliche Fixierung des Beratungsvorgangs steht damit in Widerspruch. Aus diesem Grund ist es nur dann vertretbar, daß eine Sammlung von Durchschriften von Beratungsbescheinigungen angelegt wird, wenn dafür zwingende Gründe vorgetragen werden. Dies ist bisher nicht geschehen. Die Begründung des Sozialministeriums scheint mir konstruiert und unrealistisch. Sie würde im übrigen allenfalls eine Aufbewahrung bis zu dem Zeitpunkt rechtfertigen, zu dem spätestens ein Schwangerschaftsabbruch strafrei vorgenommen werden kann. Eine Aufbewahrung zur späteren Verwendung in einem Strafverfahren ist im Hinblick auf die Verschwiegenheitspflicht des § 203 Abs. 1 Nr. 4 a StGB nicht gerechtfertigt. Gegen die Notwendigkeit der Sammlung der Durchschriften spricht auch, daß Bescheinigungen über die soziale Beratung nicht in jedem Fall ausgestellt werden müssen. Der Gesetzgeber hat bewußt darauf verzichtet, daß die soziale Beratung durch schriftliche Bestätigung nachgewiesen werden muß. Der die Schwangerschaft abbrechende Arzt darf sich nach den Regeln unseres Strafrechts mit der glaubwürdigen Zusicherung der Schwangeren über ihre Beratung zufrieden geben. Wird keine Bescheinigung ausgestellt, dann kann auch keine Durchschrift aufbewahrt und gesammelt werden. Gleichwohl dürfte auch in einem derartigen Fall die ordnungsmäßige Aufgabenerfüllung durch das Gesundheitsamt nicht gefährdet sein. Zwar verstößt die vom Sozialministerium gebilligte Praxis nicht unmittelbar gegen das Landesdatenschutzgesetz, weil es sich bei der Sammlung der Durchschriften der Beratungsbescheinigungen um eine manuell geführte Datei mit Daten, die nicht zur Übermittlung bestimmt sind, handelt und deshalb § 9 Abs. 1 LDSG keine Anwendung findet. Sie steht jedoch in erheblichen Widerspruch zu dem allgemeinen Grundsatz des Datenschutzes, daß Daten nur in dem Umfang gespeichert werden sollten, wie dies unumgänglich notwendig ist. Ich bedaure es daher sehr, daß sich das Sozialministerium noch nicht dazu entschließen konnte, eine Änderung dieser Praxis herbeizuführen.

1.1.6 Sammlung der Leichenschauschein

Nach § 22 Abs. 2 des Bestattungsgesetzes vom 21. Juli 1970 (GBl. S. 395) hat der die Leichenschau vornehmende Arzt neben einer Todesbescheinigung einen Leichenschauschein für die Todesursachenstatistik auszustellen. Diesen Leichenschauschein, dessen näherer Inhalt in der Bestattungsverordnung festgelegt ist, leitet er nach § 12 dieser Verordnung meist über das Standesamt, in bestimmten Fällen

unmittelbar dem Gesundheitsamt zu. Das Gesundheitsamt überprüft die ärztlichen Angaben des vertraulichen Teils des Leichenschauscheins auf Vollständigkeit und ergänzt sie gegebenenfalls nach Rückfrage bei dem ausstellenden Arzt. Anschließend gibt es den Leichenschauschein an das Statistische Landesamt weiter. Dieses Amt wertet die Leichenschauscheine für die Erstellung der aufgrund des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes i. d. F. vom 14. März 1980 (BGBl. S. 308) angelegten Todesursachenstatistik aus und leitet sie anschließend wieder an die Gesundheitsämter zurück. Dort werden sie mindestens fünf Jahre aufbewahrt.

Nach meinen Feststellungen erteilen die Gesundheitsämter auf Anforderung Versorgungsämtern und Trägern der gesetzlichen Unfallversicherung, insbesondere Berufsgenossenschaften, Auskunft über die Todesursache durch Übersendung einer Kopie des Leichenschauscheins. Eine Einwilligung der Angehörigen hierzu liegt häufig nicht vor. Ich halte dieses, vom Sozialministerium gebilligte Verhalten der Gesundheitsämter für rechtlich unzulässig. Die Bekanntgabe der Todesursache aus dem Leichenschauschein verletzt das Statistikgeheimnis nach § 11 Abs. 1 des Bundesstatistikgesetzes. Danach müssen Einzelangaben über persönliche und sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, von den Amtsträgern, die mit der Durchführung der Bundesstatistik betraut sind, geheimgehalten werden. Die Auffassung des Sozialministeriums, die Gesundheitsämter seien nicht mit der Durchführung der Todesursachenstatistik betraut, vermag ich nicht zu teilen. Sie läßt außer acht, daß spätestens seit dem Erlaß des Bestattungsgesetzes die Leichenschauscheine nur noch statistischen Zwecken dienen. Die Aufgabe der Gesundheitsämter besteht darin, die ärztlichen Angaben des vertraulichen Teils des Leichenschauscheins zu überprüfen und damit die Verwertbarkeit für die Todesursachenstatistik sicherzustellen. Die Weitergabe der Todesursache ohne ausdrückliche Einwilligung wäre aber auch dann unzulässig, wenn entsprechend der Rechtsauffassung des Sozialministeriums das Statistikgeheimnis von den Gesundheitsämtern nicht beachtet werden müßte. In diesem Falle würde die Datenweitergabe gegen § 10 Abs. 2 des LDSG verstoßen, da die Stellen, die um Angabe der Todesursache aus dem Leichenschauschein ersuchen, sie zu anderen Zwecken benötigen, als das Gesundheitsamt.

Meine Rechtsauffassung führt nicht dazu, daß die Stellen, die bisher um Auskunft aus den Leichenschauscheinen ersuchten, künftig ihre Aufgaben nicht mehr erfüllen können. So können z. B. die Versorgungsämter nach § 12 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung vom 6. Mai 1976 (BGBl. I S. 1169) mit Einverständnis oder auf Wunsch des Antragstellers oder der Versorgungsberechtigten von öffentlichen, freien, gemeinnützigen und privaten Krankenanstalten sowie Krankenanstalten öffentlich-rechtlicher Körperschaften und Trägern der Sozialversicherung Krankenpapiere, Aufzeichnungen, Krankengeschichten, Sektions- und Untersuchungsbefunde sowie Röntgenbilder zur Einsicht beziehen. Außerdem besteht die Möglichkeit, sich an den zuletzt behandelnden Arzt, das zuletzt behandelnde Krankenhaus oder an den Arzt zu wenden, der die Leichenschau vorgenommen hat.

1.2 Krankenhäuser

Für die dem Landesdatenschutzgesetz unterliegenden Krankenhäuser ist die Frage, unter welchen Voraussetzungen Daten von Patienten gespeichert und an Dritte übermittelt werden dürfen, von entscheidender Bedeutung. Ein kommunaler Krankenhausträger versuchte dieses Problem dadurch zu lösen, daß er entsprechend einer Musterempfehlung der baden-württembergischen Krankenhausgesellschaft in die allgemeinen Vertragsbedingungen des Krankenhauses folgende Bestimmung aufnehmen wollte: „Der Benutzer erklärt sich damit einverstanden, daß im Rahmen des mit ihm bzw. des zu seinen Gunsten abgeschlossenen Vertrags Daten über seine Person und seinen sozialen Status sowie die für seine Behandlung notwendigen medizinischen Daten gespeichert, geändert bzw. gelöscht und erforderlichenfalls, soweit nicht dadurch offenkundig seine Interessen verletzt werden, an Dritte übermittelt werden.“ Ich halte diesen Weg unter keinen Umständen für gangbar: Würde in dieser Weise verfahren, hätte ein Patient nur die Möglichkeit, entweder auf eine Aufnahme in das Krankenhaus zu verzichten oder aber die Vertragsbedingungen zu akzeptieren und damit in eine für ihn zu diesem Zeitpunkt nicht übersehbare Datenverarbeitung einzuwilligen. Da sich ein Patient häufig in einer akuten Notstandssituation befindet und darauf angewiesen ist, in das Krankenhaus aufgenommen zu werden, wäre er faktisch zu einer Einwilligung gezwungen. Eine wirksame Einwilligung nach § 5 LDSG setzt aber voraus, daß der Betroffene in der Lage ist, unter Abwägung der entstehenden Konsequenzen frei darüber zu entscheiden. Ich sehe für ein derartiges Vorgehen auch keine Notwendigkeit. Das Landesdatenschutzgesetz trägt in ausreichendem Maße den Bedürfnissen der Krankenhäuser Rechnung. Es erlaubt die Speicherung aller Daten, die zur Erfüllung der Aufgaben des Krankenhauses notwendig sind, ohne daß der Patient dazu seine Einwilligung geben müßte. Auch die Bestimmungen über die Veränderung, Sperrung und Löschung der Daten tragen den Notwendigkeiten der Krankenhäuser in ausreichendem Maße Rechnung.

Diese Überlegungen gelten im Grundsatz auch für die Weitergabe von Patientendaten an Dritte. Dabei ist allerdings neben dem Landesdatenschutzgesetz auch die Regelung über die ärztliche Schweigepflicht zu beachten. Krankenhäuser dürfen der ärztlichen Schweigepflicht unterliegende Patientendaten grundsätzlich nur mit Einwilligung des Patienten an Dritte übermitteln. Diese dem Schutz des Patienten dienende Regelung dürfen sie nicht in der Weise umgehen, daß sie die Aufnahme des Patienten in das Krankenhaus davon abhängig machen, daß er zuvor in jede Datenübermittlung an Dritte einwilligt, die nicht offenkundig seine Interessen verletzt. Wegen der Notstandssituation, in der sich ein Patient bei der Aufnahme in ein Krankenhaus befindet, kann der Abschluß eines Behandlungsvertrags grundsätzlich nicht von einer Einwilligung in nahezu alle möglichen Arten von Datenübermittlungen abhängig gemacht werden. Mit Einwilligung sollten die Krankenhäuser nur in konkreten Einzelfällen arbeiten. Dabei müssen sie den Patienten konkret darüber informieren, um welche Daten es sich handelt, an wen die Übermittlung erfolgen soll und zu welchem Zweck dies geschieht.

1.3 Krebsregister

Die Frage, ob und in welcher Form Krebsregister eingerichtet werden sollen, ist immer wieder Gegenstand der öffentlichen Diskussion. Bei uns im Lande führt der Krebsverband Baden-Württemberg e.V. bereits seit dem Jahr 1971 ein Krebsregister.

Dieses Register erfaßt bestimmte Arten von Krebserkrankungen im Regierungsbezirk Tübingen sowie in den Regionen Nord-schwarzwald und Schwarzwald-Baar-Heuberg. Grundlage für die Eintragung in das Register sind Meldungen von Ärzten und Krankenanstalten. Diese Meldungen erfolgen ohne Angabe von Name, Vorname und genauer Wohnungsanschrift (Straße und Hausnummer).

Ich halte die Führung dieses Krebsregisters für unzulässig. Die dabei praktizierte Weitergabe von medizinischen Daten ohne Einwilligung steht sowohl in Widerspruch zur ärztlichen Schweigepflicht als auch zu den Übermittlungsvorschriften des Landesdatenschutzgesetzes. Beide Regelungen finden Anwendung, obwohl bei den Meldungen keine Namensnennung erfolgt. Allein durch diese Maßnahme wird noch keine Anonymisierung erreicht, da mit Hilfe einer Reihe von Angaben auf den Erhebungs- und Mitteilungsbogen eine Identifizierung des einzelnen Patienten ohne große Schwierigkeiten möglich ist. Ich schlug deshalb dem Sozialministerium vor, dafür zu sorgen, daß die Meldungen zum Krebsregister eingestellt werden, zumal es in seiner Stellungnahme zum Ausdruck gebracht hatte, von der Weiterführung dieses Krebsregisters in der bisherigen Form sei kein wesentlicher Nutzen zu erwarten. Zu meinem Bedauern konnte sich das Sozialministerium zu diesem Schritt nicht entschließen, sondern bat um Prüfung, ob das Register nicht übergangsweise bis zum beabsichtigten Erlaß eines Krebsregistergesetzes weitergeführt werden kann. Ich bin mir durchaus bewußt, daß das Führen eines Krebsregisters mit Individualdaten, die eine Identifikation der betroffenen Personen erlauben, ein sehr vielschichtiges und kontrovers beurteiltes Problem darstellt und daß dem Datenschutz in dieser Frage immer wieder der Vorwurf gemacht wird, er behindere in unzumutbarer Weise die Krebsforschung. Ich meine jedoch, daß die derzeitige Rechtslage eine andere Beurteilung nicht zuläßt. Es ist Sache des Gesetzgebers, darüber zu entscheiden, ob eine Änderung eintreten soll. Einer solchen gesetzlichen Regelung sollte man nur nach sehr sorgfältigem Gegenüberstellen und Abwägen aller damit verbundenen Vor- und Nachteile nähertreten. Vor allem ist neben den Aspekten der medizinischen Forschung auch an das unter Umständen starke Interesse des einzelnen, durch seine Krankheit ohnehin schwer geprüften Menschen zu denken, der mit seiner Krankheit allein leben und fertig werden und nicht wider Willen Objekt medizinischer Überlegungen sein will.

1.4 Versand von ärztlichen Anamnesebogen

Es entspricht einem Grundanliegen des Datenschutzes, personenbezogene Daten nur in dem unumgänglich notwendigen Umfang zu erheben und zu sammeln. Ganz besonders sollte dies für medizinische Daten gelten. Durch eine Eingabe wurde ich auf eine städtische Kurklinik aufmerksam, deren Art von Datenerhebung diesem Grundprinzip nicht entspricht. Diese Kurklinik schickt ihren Patienten vor Kurantritt einen umfangreichen Fragebogen zu und fordert sie auf, diesen gewissenhaft auszufüllen und dem Kurarzt bei Kurantritt zu übergeben. Der Fragebogen enthält insgesamt 72 Fragen, u. a. zu jetzigen Beschwerden und Gesundheitsstörungen, zu früheren Krankheiten, Operationen und Spezialbehandlungen, Reisen in tropische Länder, Einnahme von bestimmten Präparaten und Genußmitteln, sportliche Betätigung, Krankheiten in der Familie. Ich halte diese Form von Datenerhebung für bedenklich, weil hier Patienten pauschal zur Angabe einer großen Zahl von teilweise sehr sensiblen Daten veranlaßt werden, ohne daß ein Arzt zuvor im konkreten Einzelfall die

Notwendigkeit dieser Angaben geprüft hat. Ich halte es für ausgeschlossen, daß die Kurklinik diese Angaben zur Betreuung all ihrer Patienten kennen muß. Ich empfahl deshalb der Klinik, die Anamnesebogen nicht mehr vorab zu versenden, sondern sie allenfalls bei der Untersuchung durch den Kurarzt zu verwenden, so daß dann in der verantwortlichen Entscheidung des Arztes liegt, welche Angaben zur Krankenvorgeschichte er von seinen Patienten wissen will. Inzwischen informierte mich die Klinik, sie habe den Anamnesebogen geändert und verschiedene Fragen weggelassen. Damit ist das von mir aufgeworfene Problem jedoch noch nicht befriedigend gelöst.

2. Sozialwesen

2.1 Auswirkungen der Neuregelung des Sozialgeheimnisses

Unser differenziertes, umfassendes System sozialer Leistungen macht es notwendig, daß die Sozialbehörden nahezu über jeden Bürger eine große Zahl von teilweise sehr sensiblen Informationen erheben und sammeln. Wer soziale Leistungen in Anspruch nehmen will, ist gezwungen, zum Nachweis der Leistungsvoraussetzungen Angaben zu machen, die bis in die intimsten Lebensbereiche reichen können. Derartige umfassende Datensammlungen wecken auf der einen Seite das Interesse zahlreicher Stellen. Auf der anderen Seite ist die Schutzbedürftigkeit des einzelnen Bürgers in kaum einem anderen Bereich so groß wie hier. Der Gesetzgeber versuchte zunächst, dieser Gefahrensituation durch die Schaffung des Sozialgeheimnisses in § 35 des Ersten Buchs des Sozialgesetzbuchs Rechnung zu tragen. In Form einer Generalklausel erhielt der einzelne Anspruch darauf, daß seine Geheimnisse nicht unbefugt offenbart werden. Schon bald zeigten sich jedoch in der Praxis erhebliche Schwierigkeiten bei der Anwendung dieser wenig differenzierten Regelung. Sie erwies sich als nicht geeignet, die Datenschutzprobleme befriedigend zu lösen. Zu Recht ertönte der Ruf nach einer umfassenden, auf die Besonderheiten des Sozialleistungsbereichs eingehenden Regelung des Datenschutzes. Diese brachte das SGB-Verwaltungsverfahren vom 18. April 1980 (BGBl. I S. 1469). Danach ist die Offenbarung personenbezogener Daten nur mit Einwilligung im Einzelfall oder im Rahmen einer gesetzlichen Offenbarungsbefugnis zulässig. Wann eine solche besteht, regeln im einzelnen die §§ 68 bis 77 des Zehnten Buchs des Sozialgesetzbuchs.

So sehr ich im Grundsatz den Erlaß einer bereichsspezifischen Regelung für den Bereich der Sozialdaten begrüße, so sehr muß ich andererseits betonen, daß die am Ende der letzten Legislaturperiode unter großem Zeitdruck gefundene Lösung in einer Reihe von Punkten problematisch ist. Ich halte z. B. die Amtshilferegelung zugunsten aller Behörden und sonstigen öffentlichen Stellen für zu weitgehend. Im besonderen Maße bedenklich finde ich, daß in Zukunft für alle Sozialleistungsträger ergänzend das Bundesdatenschutzgesetz gilt. Diese Regelung wird, so befürchte ich, vor allem im kommunalen Bereich erhebliche Anwendungsprobleme mit sich bringen. Die Kommunen sind in großem Umfang Träger von Sozialleistungen, z. B. auf dem Gebiet der Sozial- und Jugendhilfe, der Wohngeldleistungen und der Ausbildungsförderung. Sie haben ab 1. Januar 1981 mit Inkrafttreten der Neuregelung im Sozialleistungsbereich das Bundesdatenschutzgesetz, bei ihrer sonstigen Arbeit das Landesdatenschutzgesetz zu beachten. Einige im Landesdatenschutzgesetz enthaltene Verbesserungen gegenüber dem Bundesdatenschutzgesetz, wie etwa die Gebührenfreiheit von Auskünften über eine

Datenspeicherung, finden somit künftig ausgerechnet in dem Bereich keine Anwendung mehr, in dem das Schutzbedürfnis am größten ist.

Schon jetzt wurden an mich viele Zweifelsfragen herangetragen, die sich aus der Neuregelung des Sozialgeheimnisses ergeben. Es steht zu befürchten, daß dies nach ihrem Inkrafttreten noch in viel stärkerem Maße der Fall ist.

2.2 Datenerhebung bei Gewährung von Zuwendungen

Die Liga der freien Wohlfahrtspflege machte mich auf ein Problem aufmerksam, dem, wie auch verschiedene andere Eingaben zeigen, erhebliche Bedeutung zukommt. Soziale Einrichtungen müssen nach den Förderbestimmungen häufig, wenn sie Zuschüsse erhalten wollen, der Bewilligungsbehörde die Namen ihrer Mitarbeiter und eine Reihe weiterer Angaben zur Person mitteilen (vgl. z. B. § 4 Abs. 2 Nrn. 6—9 der Verordnung des Ministeriums für Arbeit, Gesundheit und Sozialordnung nach § 8 Abs. 5 des Kindergartengesetzes vom 9. Oktober 1980 — GBl. S. 578). In einem mir bekannten Fall des Trägers einer Wohngemeinschaft, in der psychisch Kranke und seelisch Behinderte Aufnahme finden und betreut werden, machte der überörtliche Träger der Sozialhilfe eine Förderung sogar davon abhängig, daß sowohl er als auch der Träger der örtlichen Sozialhilfe Name und eine Reihe weiterer Daten der betreuten Personen erfahren. Solche Anforderungen werden meist damit begründet, nur auf diese Weise könne eine wirksame und sparsame Mittelverwendung sichergestellt werden.

Das Landesdatenschutzgesetz findet in der Regel in derartigen Fällen keine Anwendung, da diese Vorgänge lediglich in Akten bearbeitet werden und folglich keine Datenverarbeitung in Dateien stattfindet. Aus diesem Grund kann auch § 9 LDSG, der eine Speicherung personenbezogener Daten nur dann zuläßt, wenn dies zur rechtmäßigen Aufgabenerledigung erforderlich ist, nicht unmittelbar als Beurteilungsmaßstab herangezogen werden.

Ich meine jedoch, daß man sich in diesen Fällen nicht mit einer derart formalen Betrachtungsweise zufrieden geben kann. Auch hier gilt es, dem Grundgedanken des Datenschutzes, Daten nur in dem unbedingt notwendigen Umfang zu speichern, Geltung zu verschaffen. Bei der Knappheit der öffentlichen Mittel ist es sicher ein legitimes Anliegen, Zuschüsse gezielt zu geben, um auf diese Weise mit möglichst wenig Aufwand eine möglichst große Wirkung zu erzielen. Dieses legitime Anliegen kann jedoch nicht der alleinige Maßstab für die Ausgestaltung von Förderrichtlinien sein. Vielmehr muß man auch die berechtigten Belange der Personen mit in Rechnung stellen, welche von den Fördermaßnahmen betroffen sind. Ein Weg dazu könnte sein, daß sich die Bewilligungsbehörden mehr als bisher mit Erklärungen der Zuschußempfänger begnügen und sich Kontrollen und Stichproben im Einzelfall vorbehalten. Bei einem ersten Kontakt mit dem Sozialministerium stieß ich erfreulicherweise gerade in diesem Punkt auf großes Verständnis. So liegt z. B. seinen neuen Richtlinienentwürfen über die Förderung der Ehe-, Familien- und Lebensberatungsstellen und über die Förderung von psycho-sozialen Beratungs- und ambulanten Behandlungsstellen für Suchtgefährdete und Suchtkranke bereits weitgehend dieses Prinzip zugrunde. Aber auch schon bei der Festlegung der Fördervoraussetzungen selbst sollte man so vorgehen, daß die Bewilligungsbehörde möglichst wenig personenbezogene Da-

ten über Mitarbeiter der geförderten Institutionen oder der betreuten Personen benötigt und die Zuwendungen stärker pauschaliert werden.

2.3 Sozialhilfestatistik

Die Sozialhilfestatistik wird auf der Grundlage des Gesetzes über die Durchführung von Statistiken auf dem Gebiet der Sozialhilfe, der Kriegsofopferfürsorge und der Jugendhilfe als Bundesstatistik geführt. Die Träger der Sozialhilfe müssen für diese Statistik unter anderem die Zahl der Empfänger, aufgegliedert nach Empfängergruppen und Hilfearten, mitteilen. Obwohl nach dem Gesetzeswortlaut für die Bundesstatistik nur die Zahl der Empfänger zu erfragen ist, gaben in der Vergangenheit die Träger der Sozialhilfe auf den vom Statistischen Landesamt Baden-Württemberg entworfenen Erhebungsbogen auch Name und Anschrift der Sozialhilfeempfänger an. Sie halten diese Angaben für notwendig, um Doppelerhebungen zu vermeiden und weil das Statistische Landesamt nur so die Möglichkeit habe, bei fehlerhaft ausgefüllten Erhebungsbogen zurückzufragen. Wäre diese Möglichkeit nicht gegeben, würde die Sozialhilfestatistik erheblich an Aussagekraft verlieren.

Ich halte wegen der eindeutigen Gesetzesvorschrift die Weitergabe von Name und Anschrift der einzelnen Sozialhilfeempfänger an das Statistische Landesamt nicht für zulässig. Dieses Amt teilte mir auf meine Äußerung hin mit, es teile meine rechtlichen Bedenken und werde künftig Name und Anschrift der Sozialhilfeempfänger nicht mehr erfragen. Ich begrüße diese Haltung des Statistischen Landesamts vor allem, weil es mir gerade auf dem Gebiet der Statistik notwendig erscheint, daß die Vorgaben des Gesetzgebers eingehalten werden, auch wenn dies im Einzelfall zu Lasten der Perfektion gehen kann.

3. Abschnitt: Schulen und Hochschulen

1. Schulen

1.1 Übermittlung von Schülerdaten

Zahlreiche Schulen, aber auch Eltern und private Stellen baten mich immer wieder um Auskunft, ob eine listenmäßige Weitergabe von Name und Anschrift der Schüler einzelner Klassen und ihrer Eltern zulässig ist. Insbesondere beschäftigte mich die Frage, ob die Schule den Eltern eines Schülers Name und Anschrift der Mitschüler und ihrer Eltern mitteilen darf. Ich vertrete dazu die Auffassung, daß in diesen Fällen nicht ohne Einwilligung der Schüler bzw. ihrer Eltern vorgegangen werden sollte. Datenübermittlungen an Privatpersonen und private Organisationen ohne Einwilligung läßt das Landesdatenschutzgesetz nur zu, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Eine derartige Beeinträchtigung schutzwürdiger Belange kann bei einer listenmäßigen Weitergabe der genannten Daten an Schülereltern nicht ausgeschlossen werden. Demgegenüber läßt sich nicht einwenden, bei Name und Anschrift handle es sich um Daten, die auch aus allgemein zugänglichen Quellen entnommen werden können. Diese Argumentation übersieht, daß bei einer pauschalen Weitergabe von Name und Anschrift der Schüler und ihrer Eltern auch Angaben über Familienverhältnisse und die Zugehö-

rigkeit zu einer bestimmten Schule und Schulart automatisch mitgeteilt werden. Insbesondere diese Angaben führen dazu, daß eine Beeinträchtigung schutzwürdiger Belange nicht generell ausgeschlossen werden kann. Ich begrüße das Engagement einzelner Eltern, Kontakt mit den Eltern der Mitschüler zu erhalten und möchte deshalb nicht etwa eine Kontaktaufnahme unterbinden. Auf der anderen Seite meine ich aber, daß dabei auch die Belange der Eltern respektiert werden sollten, die eine derartige Kontaktaufnahme aus verständlichen Gründen nicht wünschen. Beiden Zielsetzungen kann man am besten dadurch Rechnung tragen, daß die Eltern, z. B. im Rahmen einer Sitzung der Klassenpflegschaft, befragt werden und die Schule nur die Daten der Schüler und ihrer Eltern weitergibt, die sich damit einverstanden erklären.

1.2 Schulvergleich

Nach einer Vereinbarung der Konferenz der Kultusminister sind die Länder gehalten, Schulversuche mit Gesamtschulen einzurichten und diese wissenschaftlich zu begleiten. Im Rahmen dieser wissenschaftlichen Begleitung führt die Landesanstalt für Erziehung und Unterrichtswesen seit 1979 eine Vergleichsuntersuchung über Schulerfolg und Schulbewährung von Schülern des gegliederten reformierten Schulsystems durch. Beteiligt an der Vergleichsuntersuchung sind neben den sechs Gesamtschulen im Lande jeweils sechs ausgewählte Hauptschulen, Realschulen und Gymnasien. Als Grundlage für die Untersuchung leiten diese Schulen die dort über die Schüler vorhandenen Daten an die Landesanstalt für Erziehung und Unterricht weiter. Darüber hinaus führen sie eine Reihe von Tests durch, die dann ebenfalls die Landesanstalt für Erziehung und Unterricht auswertet. Im einzelnen handelt es sich um folgende Tests:

- Fachleistungstests, in denen die fachlichen Leistungen der einzelnen Schüler gemessen werden sollen,
- sog. Einstellungstests, die das Lern- und Arbeitsverhalten und die Einstellung des Schülers zur Schule und seinen Mitschülern zum Gegenstand haben,
- Intelligenztests, die die Grundlage für einen Vergleich von Schülern in unterschiedlich organisierten Schulen geben sollen.

In einem Elternbrief werden die Eltern über Sinn und Zweck der Vergleichsuntersuchung informiert. Auch sind darin die Maßnahmen erläutert, durch die sichergestellt werden soll, daß sämtliche gewonnenen Schülerdaten nur zum Zweck der Vergleichsuntersuchung verwendet werden dürfen. In dem Brief an die Eltern von Schülern der Schulen des gegliederten Schulsystems wird außerdem darauf hingewiesen, daß die Teilnahme an den Einstellungs- und Intelligenztests freiwillig sei. Darüber hinaus werden sie aufgefordert, der Schule auf einem beigefügten Vordruck mitzuteilen, wenn sie das Einverständnis zur Teilnahme an diesen Tests nicht geben wollen.

Die geschilderte Durchführung der Vergleichsuntersuchung verstößt unter zwei Gesichtspunkten gegen das Datenschutzrecht:

- Die Durchführung von Tests ist eine Datenerhebung im Sinne des Datenschutzrechts. Dabei muß entweder auf die Rechtsgrundlage der Erhebung oder aber darauf hingewiesen werden, daß die Angaben freiwillig sind. Der Brief an die Eltern von Schülern in Schulen des gegliederten Schulsystems trägt dieser in § 9 Abs. 2 LDSG enthaltenen Forderung nicht Rechnung, da nur die Teilnahme an den Einstellungs- und Intelligenztests als freiwillig bezeichnet wird, nicht aber die Teil-

nahme an den Fachleistungstests. Ein Schüler ist zwar grundsätzlich verpflichtet, aufgrund des Schulverhältnisses an Fachleistungstests mitzuwirken, jedoch gilt dies nur, soweit diese Tests der Erfüllung der der Schule übertragenen unterrichtlichen und erzieherischen Aufgaben dienen. Dazu zählen Leistungstests nicht, die allein zum Ziel haben, eine wissenschaftliche Untersuchung zu ermöglichen. Anders beurteilt sich die Rechtslage bei den Gesamtschulen. Bei diesen Schulen handelt es sich um Versuchsschulen im Sinne von § 22 des Schulgesetzes. Charakteristisch für derartige Schulversuche ist die Entwicklung und Erprobung neuer pädagogischer und schulorganisatorischer Erkenntnisse. Dazu gehört auch eine wissenschaftliche Begleitung und die dazu erforderliche Erhebung von Daten.

- Der Schulvergleich wird von der Landesstelle für Erziehung und Unterricht durchgeführt. Das Kultusministerium hat diese Stelle durch Erlaß dazu beauftragt. Eine derartige, die Rechtsstellung der betroffenen Schüler erheblich berührende Untersuchung kann gem. Artikel 70 Abs. 1 der Landesverfassung nicht mit einem einfachen Erlaß auf eine nachgeordnete Anstalt übertragen werden. Vielmehr bedarf es dazu einer Rechtsvorschrift. Da demzufolge keine wirksame Aufgabenübertragung stattgefunden hat, ist weder die Übermittlung der Schülerdaten von den Schulen an die Landesanstalt für Erziehung und Unterricht noch die Speicherung dieser Daten durch diese Anstalt zur rechtmäßigen Erfüllung der Aufgaben dieser Institution erforderlich. Dies bedeutet, daß die Übermittlung von Daten an die Landesanstalt für Erziehung und Unterricht und die Speicherung dieser Daten durch diese Institution in Widerspruch zu den §§ 9 und 10 LDSG stehen und deshalb unzulässig sind.

Aus diesen Gründen beanstandete ich die Durchführung der Vergleichsuntersuchung gegenüber dem Ministerium für Kultus und Sport. Das Ministerium teilte mir inzwischen mit, es sei bereit, meinen Bedenken Rechnung zu tragen. Danach wird künftig das Ministerium für Kultus und Sport die Vergleichsuntersuchungen selbst durchführen. Außerdem wird es die Eltern der Schüler von Schulen des gegliederten Schulsystems darauf hinweisen, daß auch die Teilnahme an Fachleistungstests freiwillig ist.

2. Hochschulen

Die Studenten der Hochschulen des Landes erhalten bei der Immatrikulation umfangreiche Fragebogen, die sie auszufüllen haben. Die Daten werden für Zwecke der Hochschulstatistik, zum Teil aber auch für Zwecke der Hochschule selbst benötigt. Rechtsgrundlage für die Erhebung von Studentendaten für die Hochschulstatistik sind die §§ 4 und 13 Abs. 1 Nr. 1 des Hochschulstatistikgesetzes vom 21. April 1980 (BGBl. I S. 453). Soweit Daten für Zwecke der Hochschulen erhoben werden, ist dies aufgrund der Immatrikulationsbestimmungen zulässig. Bei meinem Kontrollbesuch an der Universität Mannheim mußte ich feststellen, daß in dem von den Studenten auszufüllenden Erhebungsbogen zu Unrecht nur das Hochschulstatistikgesetz als Rechtsgrundlage angegeben war. Damit wird der unzutreffende Eindruck erweckt, sämtliche Studentendaten würden in vollem Umfang dem Statistikgeheimnis unterliegen und deshalb nicht an Dritte weitergegeben werden.

Weiter werden einige Angaben, z. B. Zahl der Kinder und angestrebtes Berufsziel, verlangt, zu deren Beantwortung die Studenten nicht verpflichtet sind, da dafür weder die Immatrikulationsbestimmungen

noch das Hochschulstatistikgesetz eine Rechtsgrundlage bieten. Diese Daten hätten demzufolge nur auf freiwilliger Basis erhoben werden dürfen. Auf diese Freiwilligkeit hätte gemäß § 9 Abs. 2 LDSG hingewiesen werden müssen. Auch das ist unterblieben.

Schließlich wurden die Studenten entgegen § 15 Abs. 4 des Hochschulstatistikgesetzes im Erhebungsbogen auch nicht darauf hingewiesen, unter welchen Voraussetzungen Einzelangaben, die für Zwecke der Hochschulstatistik gemacht wurden, an andere Stellen weitergeleitet werden dürfen.

Diese Mängel bei der Datenerhebung erscheinen mir in gewisser Weise typisch für die Datenerhebung in der Praxis. Offensichtlich wird die Unterrichtung der Bürger über die Grundlagen der Datenerhebung und ihre Folgen noch vielfach als lästige Formalie betrachtet und viel zu wenig erkannt, welche große Bedeutung der Information des Bürgers gerade bei dieser Frage zukommt.

4. Abschnitt: Steuerverwaltung

1. Anwendung des Landesdatenschutzgesetzes durch die Steuerverwaltung

1.1 Auskunft an den Bürger

Eine Grundnorm des Datenschutzes ist die in § 12 LDSG geregelte Verpflichtung der Behörden und sonstigen öffentlichen Stellen, dem Bürger auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu geben. Diese Verpflichtung ist deshalb besonders wichtig, weil durch sie der Bürger die Möglichkeit erhält, von seinen Rechten auf Berichtigung, Sperrung und Löschung von personenbezogenen Daten Gebrauch zu machen.

Die Auskunftspflicht erfährt allerdings eine gewisse Einschränkung durch § 12 Abs. 2 LDSG. Die in dieser Bestimmung genannten Behörden, zu denen neben der Polizei u. a. auch Behörden zählen „soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern“, müssen nicht in jedem Falle einem Auskunftsantrag entsprechen; sie haben darüber vielmehr nach pflichtgemäßem Ermessen zu entscheiden. Keinesfalls kann, wie dies immer wieder geschieht, aus § 12 Abs. 2 LDSG der Schluß gezogen werden, im Anwendungsbereich dieser Bestimmung könne ohne weiteres eine Auskunft verweigert werden.

Nach Auffassung des Finanzministeriums fallen unter diese das Auskunftsrecht des Bürgers einschränkende Regelung alle Behörden der Steuerverwaltung, soweit sie im Rahmen der Steuerfestsetzung und Steuererhebung Daten speichern. Dasselbe soll auch für die Speicherung personenbezogener Daten durch Dienstvorgesetzte, Dienstaufsichtsbehörden und Rechnungsprüfungsbehörden im Rahmen ihrer Aufsichtstätigkeit gelten. Im Ergebnis bedeutet dies, daß nahezu die gesamte Steuerverwaltung Auskünfte nur im Rahmen ihres pflichtgemäßen Ermessens erteilen müßte. In Übereinstimmung mit den anderen Landesbeauftragten für den Datenschutz und dem Bundesbeauftragten für den Datenschutz vermag ich diese Auffassung nicht zu teilen. Zwar wäre es wohl zu eng, wenn nur bei Dateien der Steuerfahndung oder der Betriebsprüfung die Auskunftspflicht eingeschränkt wäre. Doch muß auf der anderen Seite bedacht werden, daß § 12 LDSG einen Auskunftsanspruch nicht bei jeder Datenspeicherung, die eine Behörde in Erfüllung ihrer gesetzlichen Aufgaben im An-

wendungsbereich der Abgabenordnung vornimmt, einschränkt. Eine abschließende Beurteilung wird letztlich nur unter Berücksichtigung der konkreten Zweckbestimmung der einzelnen Dateien möglich sein. Diese Frage, die im Hinblick auf § 17 Abs. 2 LDSG auch Bedeutung für die Führung des Datenschutzregisters hat, wird im kommenden Jahr Gegenstand eingehender Erörterungen mit dem Finanzministerium sein.

Die restriktive Haltung des Finanzministeriums in dieser Frage erfährt zusätzliche Bedeutung dadurch, daß dieses Ministerium die nachgeordneten Behörden angewiesen hat, in den Fällen des § 12 Abs. 2 LDSG keinerlei Auskunft zu geben. Ich halte diese Anweisung nicht nur für rechtlich fehlerhaft, da durch sie die nachgeordneten Behörden angewiesen werden, von einem ihnen eingeräumten Ermessensspielraum in keinem Fall zu Gunsten des Bürgers Gebrauch zu machen. Sie erscheint mir auch aus rechtspolitischen Gründen äußerst bedenklich, weil sie sicherlich nicht dazu beiträgt, das Vertrauen des Bürgers in die Verwaltung zu stärken. Die in § 12 Abs. 2 LDSG getroffene Regelung trägt der besonderen Aufgabenstellung der dort genannten Behörden Rechnung. Diese erfordert keinesfalls, daß in jedem Fall von einer Auskunftserteilung abgesehen wird. Vielmehr ist anzunehmen, daß es zahlreiche Fälle gibt, in denen das Auskunftsinteresse des Bürgers das öffentliche Interesse an der Geheimhaltung überwiegt.

1.2 Steuergeheimnis

Eine ähnlich restriktive Haltung wie beim Auskunftsrecht nach § 12 LDSG nimmt das Finanzministerium auch gegenüber meiner Überwachungstätigkeit ein. Sie geht davon aus, daß das Steuergeheimnis (§ 30 AO) auch gegenüber dem Landesbeauftragten für den Datenschutz bei dessen Überwachungstätigkeit zu beachten ist. Ich halte diese Auffassung nicht für zwingend. Sie würde meine Überwachungstätigkeit in einem wichtigen Bereich empfindlich einschränken. Denn sie würde praktisch dazu führen, daß ich nur noch tätig werden könnte, wenn sich ein Steuerpflichtiger bei mir beschweren würde. Ich könnte kaum noch Kontrollen von Amts wegen durchführen, die über eine Überprüfung von allgemeinen Datensicherungsmaßnahmen hinausgehen und die ich für unverzichtbar halte. Ich werde mich deshalb darum bemühen, mit der Steuerverwaltung zu einer für beide Seiten tragbaren Lösung zu kommen.

1.3 Verwendung von Adreßaufklebern

Durch eine Eingabe bin ich darauf aufmerksam gemacht worden, daß ein Finanzamt im Bezirk der Oberfinanzdirektion Stuttgart einen Adreßaufkleber verwendet hat, aus dem ohne Schwierigkeiten die Geburtstage der steuerpflichtigen Eheleute, die Religionszugehörigkeit und die Steuernummer zu ersehen waren. Das Finanzamt hat mir mitgeteilt, daß es sich dabei um ein Versehen gehandelt habe und dieser Mangel sofort abgestellt worden sei. Die eigentlichen Adreßaufkleber enthielten bei allen Finanzämtern der Oberfinanzdirektion Stuttgart außer der Anschrift nur noch die Steuernummer des jeweiligen Steuerpflichtigen. Ich halte auch dieses Verfahren für fragwürdig. Durch die Angabe der Steuernummer auf Adreßaufkleber wird es einem Unbefugten ermöglicht, telefonisch Auskunft über die persönlichen und sachlichen Verhältnisse eines Steuerpflichtigen jedenfalls dann zu erhalten, wenn die Befragung geschickt genug erfolgt. Ich gehe selbstverständlich davon aus, daß die Bediensteten der Finanzämter bei der Erteilung von telefonischen Aus-

künftigen Vorsicht walten lassen, meine jedoch, daß eine derartige Mißbrauchsmöglichkeit von vornherein ausgeschlossen werden sollte. Aus diesem Grund habe ich bereits im August das Finanzministerium gebeten, eine Änderung des derzeitigen Verfahrens herbeizuführen. Leider hat das Finanzministerium dazu bisher noch nicht Stellung genommen.

5. Abschnitt: Allgemeine Verwaltung

1. Personalwesen

1.1 Führung von Personalkarteien

Nach meinen Beobachtungen führen die Behörden häufig neben den Personalakten über die Beamten noch Personaldateien in Form von Karteien. Ihr Inhalt ist unterschiedlich. Zum Teil enthalten sie nur die Grunddaten wie Name, Amtsbezeichnung, Geburtstag und Anschrift, zum Teil jedoch auch die gesamten Personalien, Angaben über den beruflichen Werdegang, die Prüfungs- und Beurteilungsnoten, Beförderungen, Abordnungen, Versetzungen, Disziplinarmaßnahmen. Solche Personalkarteien sind auch Personalakten mit der Folge, daß die Grundsätze des Beamten- und Tarifrechts, wie zum Beispiel das Prinzip der Vertraulichkeit und Einsichtsrecht des Beamten, für sie gelten. In der Regel existieren solche Karteien bei den personalverwaltenden Stellen. Zu meiner Überraschung stellte ich bei einer Kontrolle fest, daß der Leiter des Verkehrsdienstes einer Polizeidienststelle über seine 43 Mitarbeiter eine Personalkartei mit zahlreichen Angaben, z. B. auch über Schulbildung, erlernten Beruf, besondere Sprachkenntnisse, Teilnahme an Lehrgängen, Fehlzeiten wegen Erkrankung, Beförderungen und sonstige Laufbahn, führt. Weil der Leiter des Verkehrsdienstes nicht für die Personalverwaltung, sondern für ganz andere Aufgaben zuständig ist, halte ich diese Kartei für unzulässig. Ich habe die Polizeidienststelle gebeten, sie umgehend zu vernichten.

1.2 Automatisierte Verfahren zur Unterstützung der Personalverwaltung

Wie in der privaten Wirtschaft sind auch im Bereich der öffentlichen Verwaltung Bestrebungen erkennbar, sich bei der Personalverwaltung und -planung der Hilfe der automatisierten Datenverarbeitung zu bedienen. So wird derzeit bei der Oberfinanzdirektion Freiburg ein „automatisiertes Verfahren zur Unterstützung der personalverwaltenden Stellen der Oberfinanzdirektionen (UPS)“ erprobt. Über seine endgültige Einführung will man nach seiner Erprobung entscheiden. Derartige Verfahren werfen eine Reihe von Fragen auf:

- Ein wesentlicher Punkt ist das Verhältnis dieser Verfahren und der dabei entstehenden Personaldateien zu den Personalakten. Nach den beamten- und tarifrechtlichen Bestimmungen haben die Bediensteten ein umfassendes Recht auf Einsicht in die Personalakten. Zur Sicherung dieses Rechts bestimmt § 113 Abs. 4 Satz 1 LBG, daß über die Beamten bei einer Behörde oder Dienststelle keine weiteren Akten geführt werden dürfen. Da in in automatisierten Verfahren betriebene Dateien keine Einsicht genommen, sondern nur Auskunft gegeben werden kann, stellt sich die Frage, ob solche Daten bei der derzeitigen gesetzlichen Regelung der Personalaktenführung überhaupt geführt werden dürfen.

- Unabhängig von dieser Grundsatzfrage muß sichergestellt sein, daß sich die Personalverwaltung stets der beschränkten Aussagekraft derartiger Dateien bewußt ist. Da bei Personalentscheidungen die Persönlichkeit der einzelnen Bediensteten umfassend zu würdigen ist, dürfen sie nicht allein auf der Grundlage der kein vollständiges Bild des Bediensteten wiedergebenden Personaldateien getroffen werden. Hierfür sind stets die Personalakten zuzuziehen und zu nutzen.
- Der Grundsatz der Vertraulichkeit ist in gleicher Weise wie beim Führen von Personalakten auch bei der Führung automatisierter Personaldateien zu beachten. Dies macht es notwendig, die Zugriffsbefugnisse auf die Personaldatei genau festzulegen und eng zu begrenzen. Durch technische und organisatorische Maßnahmen ist dafür zu sorgen, daß diese Zugriffsregelungen nicht umgangen werden können.
- Die durch den Einsatz der EDV gegebene Möglichkeit darf im übrigen nicht dazu führen, anderen als der personalaktenführenden Stelle einen unmittelbaren Zugriff auf die Personaldateien zu geben. Andernfalls würden die Zuständigkeitsregelungen für die Personalaktenführung in Frage gestellt werden. Hätte z. B. ein Ministerium jederzeit eine unbeschränkte Zugriffsmöglichkeit zu sämtlichen Daten sämtlicher Bediensteter der ihm nachgeordneten Behörden, dann stünde die Regelung, durch die die Zuständigkeit für die Personalaktenführung auf nachgeordnete Behörden übertragen wurde, weitgehend auf dem Papier. Damit will ich keinesfalls das Recht des Ministeriums, im Einzelfall aus konkretem Anlaß die Übermittlung von Daten zu verlangen, in Frage stellen. Ein berechtigtes Interesse eines Ministeriums an einer ständigen Übermittlung sämtlicher gespeicherter Daten aller Bediensteten vermag ich jedoch nicht zu erkennen.

1.3 Registrierung dienstlicher und privater Telefongespräche

In Baden-Württemberg registriert die Landesverwaltung bei dienstlichen und privaten Ferngesprächen über Dienstapparate u. a. Datum und Uhrzeit des Gesprächs und die gewählte Rufnummer.

- Bei Dienstgesprächen ist diese Art der Datenspeicherung kaum problematisch. Denn die Registrierung der genannten Daten berührt nach herrschender Meinung den Schutzbereich des durch Art. 10 GG gewährleisteten Grundrechts auf Einhaltung des Fernmeldegeheimnisses nicht. Die Speicherung ist im übrigen erforderlich, um der Dienststelle die Möglichkeit zu Kontrollen darüber zu geben, ob die Grundsätze der Wirtschaftlichkeit und Sparsamkeit (§ 7 Abs. 1 LHO) beachtet worden sind.
- Anders beurteilt sich die Rechtslage bei privaten Ferngesprächen. Bei solchen Gesprächen ist Artikel 10 GG in vollem Umfang zu beachten. Eine Registrierung von genauer Zeit und gewählter Rufnummer ohne Verstoß gegen Artikel 10 GG ist hier grundsätzlich nur mit Einwilligung des Bediensteten möglich. Wegen dieser Rechtslage muß die Landesverwaltung mindestens folgendes Verfahren beachten: Sie muß die Bediensteten darüber informieren, unter welchen Voraussetzungen sie den Dienstapparat für private Ferngespräche benutzen können. Insbesondere hat sie anzugeben, welche Daten im einzelnen gespeichert werden. Der einzelne Bedienstete kann dann frei entscheiden, ob er unter diesen Umständen von seinem Dienstapparat aus ein Privatgespräch führen will. Tut er dies, liegt darin auch eine Einwilligung in die

Registrierung. Sie schließt einen Verstoß gegen Artikel 10 GG aus wie auch das Landesdatenschutzgesetz bei dieser Verfahrensweise nicht verletzt wird. Es läßt eine solche Datenspeicherung zu, weil sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Mit der Benützung des Dienstapparats zu privaten Ferngesprächen kommt eine vertragliche Vereinbarung zwischen Dienststelle und Gesprächsteilnehmer zustande. Die Registrierung ist zur Vertragsabwicklung erforderlich. Sie ermöglicht der Dienststelle, ihre sich aus der vertraglichen Vereinbarung ergebende Entgeltforderung geltend zu machen. Dazu ist sie auf die Kenntnis der gewählten Rufnummer und den Zeitpunkt des Gesprächs zumindest solange angewiesen, als ein Dienstapparat von verschiedenen Personen benutzt werden kann. Dieses Bedürfnis für eine Speicherung entfällt jedoch spätestens mit der Einziehung des Entgelts. Ab diesem Zeitpunkt werden die gespeicherten Daten nicht mehr zur Aufgabenerfüllung benötigt. Sie müssen deshalb gemäß § 12 Abs. 2 LDSG gesperrt werden. Zu einer Löschung zwingt das Landesdatenschutzgesetz ohne Antrag des Betroffenen nicht; sie wäre jedoch unter dem Aspekt des Datenschutzes generell wünschenswert.

2. Kommunale Angelegenheiten

2.1 Nutzen von Unterschriftenlisten für Bürgerbegehren zu anderen Zwecken

Eine Eingabe betraf die Verwendung der Unterschriftenlisten für ein Bürgerbegehren. Ein Bürgermeisteramt wandte sich anhand dieser Liste an die unterzeichnenden Bürger und übersandte ihnen ein Informationsblatt über seine abweichende Meinung. Zu diesem Zweck ließ es die Namen der Unterzeichner vorübergehend im regionalen Rechenzentrum speichern. Diese Speicherung war nach § 9 Abs. 1 LDSG unzulässig, weil sie nicht zur rechtmäßigen Erfüllung der Aufgaben der Gemeinde erforderlich war. Auch halte ich die erfolgte Nutzung der Unterschriftenliste durch das Bürgermeisteramt wegen der Regelung des § 15 a der Kommunalwahlordnung für bedenklich. Nach dieser Regelung dürfen die Unterschriften für ein Bürgerbegehren nur Behörden und sonstigen Stellen überlassen werden, soweit es die Durchführung des Bürgerbegehrens erfordert. Es spricht vieles dafür, daß diese Regelung andere Datenübermittlungen aus dieser Liste ausschließen wollte. Das Innenministerium erklärte sich auf meinen Vorschlag bereit, dies bei der nächsten Novellierung des Kommunalwahlrechts klarzustellen.

2.2 Vergabe von Grundstücken

Die gegenwärtige Situation auf dem Grundstücksmarkt stellt die Gemeinden bei der Vergabe von Bauland vor die Notwendigkeit, unter zahlreichen Bewerbern eine Auswahl zu treffen. In einem mir bekannten Fall verlangte eine Gemeinde von den Bauinteressenten neben Angaben zu ihren persönlichen und wirtschaftlichen Verhältnissen getrennt für die Ehegatten auch Angaben über deren politisches, kirchliches und gesellschaftliches Engagement.

Solche Aktionen finden ihre absolute Schranke im Verfassungsgebot des Art. 3 Abs. 3 GG, wonach niemand wegen seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen und politischen Anschauungen benachteiligt oder bevorzugt werden darf. Ebenso zieht Artikel 140 GG in Verbindung mit Artikel 136 Abs. 3 der Weimarer Verfassung eine

klare Schranke dadurch, daß niemand verpflichtet ist, seine religiöse Überzeugung zu offenbaren. Außerdem ist die Rechtsprechung des Bundesverfassungsgerichts zu bedenken, wonach Differenzierungen einen vernünftigen, sachlich einleuchtenden Grund voraussetzen. Innerhalb dieser Grenzen sind Gemeinden befugt, Bauinteressenten nach Umständen zu fragen, die bei der Auswahl der Bewerber zur Entscheidungsfindung herangezogen werden können. So kann man sicherlich die persönlichen und wirtschaftlichen Verhältnisse eines Bewerbers und seine Verdienste um eine Gemeinde bei der Entscheidung berücksichtigen. Bedenklich sind jedoch gezielte Fragen zum persönlichen Engagement, denen sich der Bewerber nicht entziehen kann, wenn er Nachteile vermeiden will. Auf solche sollten die Gemeinden verzichten.

2.3 Akten über Einwohner

Das Bürgermeisteramt ist die Behörde, mit der der Bürger am meisten in Verbindung tritt. Vor allem kleinere Gemeinden führen eine Akte, in der die ganzen Kontakte registriert sind. Diese sog. Personalakten sind alphabetisch geordnet. Teilweise werden Vorgänge familienweise zusammengefaßt. In den Akten befinden sich Unterlagen aus fast allen Lebensbereichen, insbesondere Anträge des Einwohners und Bescheide nicht nur des Bürgermeisteramts, sondern auch zahlreicher anderer Behörden. In einem Fall fand ich in den Akten sogar noch Strafnachrichten, Erklärungen über den Zeitpunkt des Beitritts zur NSDAP und Spruchkammerbescheide. Eine Bereinigung der Akten findet nach Angaben der Bürgermeisterämter entweder nur in sehr langen Zeitabständen oder gar erst nach dem Tod der Betroffenen statt.

Die Anlegung derartiger Sammelakten mag aus der Sicht der Gemeinden zweckmäßig sein. Sie verstößt auch nicht gegen eine Rechts- oder Verwaltungsvorschrift. Niemand wird andererseits bestreiten wollen, daß solche Sammlungen schutzwürdige Belange der Bürger beeinträchtigen können. Je länger die Akten aufbewahrt und je mehr Vorgänge in sie aufgenommen werden, desto mehr eignen sie sich für einen Mißbrauch. Sie ermöglichen der Behörde oder ihren einzelnen Bediensteten, über einen Bürger ein umfassendes Persönlichkeitsprofil zu erstellen. Ich habe deshalb den kommunalen Landesverbänden nahegelegt, ihren Gemeinden zu empfehlen, solche Sammlungen in regelmäßigen, nicht zu langen Zeitabständen zu bereinigen.

3. Aktenaussonderung und Archivverwaltung

Zu den althergebrachten Grundsätzen unserer Verwaltung gehört, daß sie Daten und Vorgänge, die sie einmal gesammelt hat, auch solange wie möglich aufbewahrt. Die einzige Schranke bildeten bisher die räumlichen und personellen Verhältnisse der einzelnen Registraturen. Der Gedanke, daß durch das Aufbewahren von Informationen berechnete Interessen von Personen gefährdet sein könnten, war der Verwaltung bisher weitgehend fremd. Die bestehenden Vorschriften über die Aktenaussonderung und Aktenvernichtung regeln nur, unter welchen Voraussetzungen Unterlagen ausgesondert und vernichtet werden dürfen, nicht aber, unter welchen Voraussetzungen dies geschehen muß. Ich halte es für eine wichtige Aufgabe, eine Änderung dieser Praxis herbeizuführen. Dem Grundgedanken des Datenschutzes, daß Daten nur so lange aufbewahrt werden sollten, als sie zur Aufgabenerfüllung benötigt werden, ist stärker als bisher Geltung zu verschaffen. Es gilt, der gelegentlich zu beobachtenden Mentalität, allenfalls das zu tun, wozu das Landesdatenschutzgesetz ausdrücklich verpflichtet, entgegenzutreten und offen-

siv den Gedanken des Datenschutzes auch bei den Verwaltungsvorgängen Geltung zu verschaffen, auf die das Landesdatenschutzgesetz nicht unmittelbar Anwendung findet. Nicht zu leugnen ist, daß diese Zielsetzung in einem gewissen Gegensatz zu den Interessen der Archivverwaltung steht, zeitgeschichtlich bedeutsame Vorgänge aufzubewahren und der Forschung zur Verfügung zu stellen. Wegen dieser unterschiedlichen Interessenlage muß man nach einer Lösung suchen, die einerseits den berechtigten Belangen der Betroffenen Rechnung trägt, die es auf der anderen Seite aber auch der Archivverwaltung ermöglicht, ihrer Aufgabe gerechtzuwerden.

4. Statistik

Der große Bedarf an Statistiken ist ein Charakteristikum unserer Zeit. Politik, Verwaltung und Wirtschaft legen Wert auf Statistiken, um Grundlagen für ihre Entscheidungen zu erhalten oder aber um die Richtigkeit bereits getroffener Entscheidungen unter Beweis zu stellen. Zur Erstellung derartiger Statistiken werden im großen Umfang personenbezogene Daten erhoben, sei es durch Befragen des Betroffenen selbst, sei es durch Befragen anderer Personen und Stellen. Der Bürger wird damit zum staatlichen Informationsobjekt. Den sich aus einer derart umfangreichen Datenbeschaffung ergebenden Gefahren für den betroffenen Bürger begegnete der Gesetzgeber durch die Schaffung des Statistikgeheimnisses im Bundesstatistikgesetz. Mit dieser sicherlich sehr begrüßenswerten Regelung können wir uns jedoch nicht zufrieden geben. Das Statistikgesetz gilt nur für die Erstellung von Bundesstatistiken. Zu prüfen ist, ob nicht im Landesrecht eine entsprechende Regelung erlassen werden muß. Der wirksamste Datenschutz besteht im übrigen darin, möglichst wenig personenbezogene Daten zu erheben und zu speichern. Dies macht es notwendig, nach weiteren Verfahren zur Anonymisierung zu suchen. Weiter gilt es sicherzustellen, daß auch nicht aus Gründen der Verwaltungsvereinfachung den mit der Erstellung der Statistiken befaßten Stellen mehr Daten zugehen, als benötigt werden. Schließlich ist zu überlegen, ob nicht unter Verzicht auf absolute Perfektion von der Erhebung solcher Daten abgesehen werden kann, die bisher lediglich zu Kontrollzwecken dienen und Rückfragen ermöglichen sollen.

6. Abschnitt: Datenverarbeitung

1. Stand der Datenverarbeitung

Die meiner Überwachung unterliegenden Behörden und sonstigen öffentlichen Stellen setzen in sehr unterschiedlichem Maße die automatisierte Datenverarbeitung (ADV) ein. Verwaltungsbereiche, in denen weitgehend manuelle Datenverarbeitung stattfindet, stehen anderen Bereichen gegenüber, in denen in großem Umfang die ADV eingesetzt wird. Erhebliche Bedeutung hat die ADV insbesondere in der Steuerverwaltung, im Besoldungswesen, in der Statistik, im Sicherheitsbereich, in der Versorgungs- und Sozialverwaltung, bei den Vermessungsbehörden, in der Hochschul- und Schulverwaltung und im Gebäudeversicherungswesen. Ebenso gibt es auf kommunaler Ebene zahlreiche landeseinheitliche Verfahren, die in den Regionalen Rechenzentren zur Verfügung stehen und von der überwiegenden Zahl der Kommunen genutzt werden. Erwähnenswert sind hier vor allem die automatisierten Verfahren im Einwohnerwesen, im Personalwesen und im kommunalen Finanzwesen. Einige wenige Kommunen betreiben über kleine EDV-Anlagen eigene Verfahrensentwicklungen oder bedienen sich der in Service-Rechenzentren angebotenen Verfahren.

In welchem Maße ein Bürger allein vom Einsatz der automatisierten Datenverarbeitung durch seine Heimatgemeinde betroffen sein kann, mag folgendes Beispiel zeigen: Für jeden Bürger werden im Einwohnerwesen ca. 40 Stammdaten gespeichert, darunter Name, Anschrift, Geburtsort, Staatsangehörigkeit und Religionszugehörigkeit. Ist dieser Bürger z. B. Grundbesitzer, Gewerbesteuer- und feuerwehrgabepflichtig, Hundehalter, Zahler von Müllabfuhrgebühren, Abnehmer von Leistungen der Stadtwerke, in einem städtischen Krankenhaus zeitweise Patient und muß er außerdem sonstige Zahlungen an die Gemeinde leisten, können allein im kommunalen Finanzwesen ca. 400 weitere Daten hinzukommen. Diese könnten, würden sie über einen gemeinsamen Ordnungsbegriff verknüpft, durchaus als Grundlage für die Erstellung eines umfassenden Persönlichkeitsprofils dieses Bürgers verwendet werden.

2. Weiterentwicklung der automatisierten Datenverarbeitung

Alle Bereiche der öffentlichen Verwaltung treiben die Entwicklung von automatisierten Verfahren ständig voran. Aus dem kommunalen Bereich sind Verfahren für die Kfz-Zulassung, die Abwicklung der Sozialhilfezahlungen und das Bußgeldverfahren erwähnenswert. Im staatlichen Bereich stehen neben Planungen von Personalinformationssystemen vor allem das gerichtliche Mahnverfahren und das automatisierte Liegenschaftsbuch im Vordergrund. Bei Verfahrensweiter- und -neuentwicklungen geht die Entwicklung zunehmend dahin, dem Anwender den Direktzugriff auf die gespeicherten Daten über Bildschirm und Leitung zu ermöglichen. Ziel ist, auf diese Weise über die Daten rascher verfügen und dadurch auch dem Bürger schneller Auskunft geben zu können.

3. Datensicherung

Wirksamer Datenschutz ist ohne Datensicherung nicht möglich. Unter Datensicherung sind dabei alle technischen und organisatorischen Maßnahmen zu verstehen, die geeignet und geboten sind, den Bestand, Inhalt und die Organisation der Daten sowie die Programme und EDV-Anlagen gegen unberechtigten Zugriff und vor Mißbrauch zu schützen sowie vor Verlust und Zerstörung zu bewahren. Welche Anforderungen an die Datensicherung zu stellen sind, ist in § 8 LDSG und in der Anlage zum Landesdatenschutzgesetz nur sehr abstrakt festgelegt. Nicht zuletzt aus diesem Grunde tun sich die einzelnen Behörden oft schwer, im Einzelfall festzustellen, welche konkreten Sicherungsmaßnahmen getroffen werden müssen. Hinzu kommt, daß die Verwirklichung von Datensicherungsmaßnahmen weniger in der manuellen als in der automatisierten Datenverarbeitung zu Erschwernissen im Arbeitsablauf führen kann. Nicht selten kann sie auch mit erheblichen Kosten verbunden sein. Auch aus diesem Grunde unterbleiben häufig an sich gebotene Datensicherungsmaßnahmen.

3.1 Datensicherung in der manuellen Datenverarbeitung

Die Vielfalt der Organisationsformen der vom Landesdatenschutzgesetz erfaßten öffentlichen Stellen und die unterschiedlichen örtlichen und baulichen Gegebenheiten lassen einheitliche Aussagen über Art und Umfang der Datensicherungsmaßnahmen kaum zu. Trotz dieser Schwierigkeiten halte ich gleichwohl die Erfüllung folgender Mindestanforderungen für geboten:

— Aufbewahrung der Dateien

Dateien sollten grundsätzlich in abschließbaren Behältnissen oder Räumen aufbewahrt werden. Je nach dem Grad der Sen-

sitivität der gespeicherten Daten müssen zusätzliche Anforderungen an die Behältnisse, in denen die Dateien aufbewahrt werden, gestellt werden. Durch organisatorische Regelungen ist sicherzustellen, daß nur in Anwesenheit eines Bediensteten auf die Datei zugegriffen werden kann. Ist dies nicht der Fall, müssen die Behältnisse oder die Räume, in denen die Dateien aufbewahrt werden, verschlossen sein. Auch muß jederzeit festgestellt werden können, wer Schlüssel für die Räume oder Behältnisse besitzt, in denen Dateien aufbewahrt werden. Die Behörde sollte möglichst wenig Schlüssel ausgeben. Werden Dateien in Räumen, in denen ein erheblicher Publikumsverkehr stattfindet, geführt, ist eine Trennung von Besucher- und Bearbeitungszonen geboten.

— Zugriff zu Dateien

Insbesondere größere Behörden sollten durch organisatorische Regelungen genau festlegen, welche Bediensteten auf die Dateien zugreifen können.

3.2 Datensicherung in der automatisierten Datenverarbeitung

In der automatisierten Datenverarbeitung wird Datensicherung schon seit längerem betrieben, und zwar nicht zuletzt im Interesse der datenverarbeitenden Stellen selbst. Das Bewußtsein für ihre Notwendigkeit ist dort deshalb stärker entwickelt. Auch sind die zu erfüllenden Anforderungen in der Anlage zu § 8 LDSG stärker konkretisiert als bei der manuellen Datenverarbeitung. Wie die verschiedenen Kontrollbesuche in Rechenzentren zeigten, sind gleichwohl auch in diesem Bereich eine Reihe typischer Mängel festzustellen:

— Organisatorische Regelungen

Jedes Rechenzentrum sollte unbedingt in einer schriftlichen Anleitung festlegen, wer welche einzelnen Aufgaben im Rahmen der Datenverarbeitung zu erfüllen hat, und die ordnungsgemäße und sichere Abwicklung der automatisierten Verfahren regeln. Leider mußte ich feststellen, daß solche Anleitungen teilweise veraltet, oft aber gar nicht schriftlich getroffen sind. Außerdem tragen auch häufig neuere Regelungen den Anforderungen des Datenschutzes zu wenig Rechnung.

— Programmentwicklung und Programmpflege

Die Vergabe von Programmieraufträgen für neue Programme oder zur Änderung bestehender Programme ist vielfach unzureichend geregelt. Oft fehlt eine zentrale Stelle innerhalb der Behörde, die diese Aktivitäten überwacht. Folglich würde es gar nicht auffallen, wenn Programmierer eigenmächtig Programme erstellen oder ändern. Dies wiegt besonders schwer, wenn außerdem nicht einmal, wie ich auch feststellen mußte, ein Programmverzeichnis vorhanden und folglich auch nicht festzustellen ist, welche Programme in dem Rechenzentrum überhaupt eingesetzt werden dürfen.

— Programmtests mit aktuellen Daten

In einigen Rechenzentren war zu bemängeln, daß Testarbeiten nahezu ausschließlich mit „echten“ Daten durchgeführt wurden. Solche Programmtests gefährden die Verfahrenssicherheit im Rechenzentrum: Programmierer erhalten unbeeinträchtigt Zugang zu personenbezogenen Daten. Außerdem können die Testergebnisse in die Fachabteilungen gelangen und dort als normale Arbeitsergebnisse verarbeitet werden. Aus diesen Gründen halte ich es grundsätzlich für erforderlich,

daß Programmtests nur mit anonymisierten Daten durchgeführt werden. Dabei verkenne ich nicht, daß sich Tests mit aktuellen Daten nicht ganz vermeiden lassen. Dies sollte aber nur im Einzelfall aufgrund schriftlicher Genehmigung des Behördenleiters oder eines von ihm Beauftragten möglich sein.

— Kontrolle der Datenverarbeitung

Nahezu alle Rechenzentren setzen Verfahren ein, die die Vollständigkeit und Richtigkeit des Ablaufs einzelner Programme automatisch nachweisen und eine Vielzahl gezielter Auswertungen zulassen. Diese Auswertungen und Protokolle werden zwar häufig auch erstellt, aber selten überprüft. Hier besteht die Gefahr, daß während der Verarbeitung aufgetretene Fehler nicht entdeckt werden, Programme mehrmals oder unberechtigt ablaufen und Datenträger mit personenbezogenen Daten dupliziert werden, ohne daß man dies bemerkt.

— Kontrolle der Datenarchive

Erfreulicherweise sehen die meisten der von mir bislang kontrollierten Stellen automatisierte Verfahren zur Verwaltung der Magnetbandbestände vor. Diese ermöglichen eine anonyme Beschriftung und eine Vielzahl von Auswertungen über den Einsatz der einzelnen Magnetbänder. Leider werden die Auswertungsmöglichkeiten zwar genutzt, die Ergebnisse aber nur in wenigen Fällen regelmäßig und gezielt überprüft. Dies aber ist notwendig, um die Vollständigkeit des Datenarchivs zu gewährleisten.

Neue Probleme der Datensicherung wirft der vermehrte Einsatz der Datenfernverarbeitung auf. Sie ermöglicht dem Benutzer einen direkten Zugriff über Leitung und Bildschirm auf die entfernt gespeicherten Daten. Die Kontrollfunktionen des Rechenzentrums sind dadurch weitgehend ausgeschaltet; insbesondere entfallen die visuellen Kontrollen. Diese Kontrollfunktionen müssen durch andere technische Maßnahmen ersetzt werden. Deshalb ist sicherzustellen, daß nur befugte Personen zum Datenverarbeitungssystem Zugang haben und daß sie weder unbeabsichtigt noch gezielt auf fremde Bereiche und Daten zugreifen können. Meine Kontrollen haben auch hier einige Schwachstellen aufgezeigt:

— Mechanische Sicherung der Bildschirme

Eine große Zahl von Bildschirmen war nicht mit einem Betriebsschloß ausgestattet und die Gefahr der unbefugten Benutzung dadurch gegeben. Zumindest die Bildschirme, über die personenbezogene Daten abgerufen werden können, sollten durch ein Betriebsschloß oder durch andere Einrichtungen, z. B. durch Ausweislesesysteme, gesichert sein.

— Benutzer- und Zugriffskontrolle

Bei einem Kontrollbesuch mußte ich feststellen, daß an sämtlichen Bildschirmen die Einrichtung zum Unsichtbarmachen der Benutzerkennwörter, die den unberechtigten Abruf von Daten eigentlich verhindern sollen, fehlt. Da auch der Zugang zu den Bildschirmen kaum eingeschränkt ist, besteht die akute Gefahr eines Datenmißbrauchs. In einem Verfahren war die Sicherung der Daten gegen mißbräuchliche Nutzung durch den Einsatz von Kennwörtern überhaupt nicht vorgesehen. Mit dem Öffnen des Betriebsschlusses und Aufruf des Dialogprogramms standen die über den betreffenden Bildschirm abrufbaren Daten allen Bediensteten, die Zugang zu diesem Bildschirm hatten, zur Verfügung. In einem weiteren Fall

stellte ich fest, daß trotz der Vergabe von Benutzerkennwörtern die Daten nicht hinreichend geschützt sind. Dort ist es bis jetzt möglich, mit Hilfe dieser Kennwörter von jedem an dem Datenverarbeitungssystem angeschlossenen Bildschirm auf die geschützten Daten und Programme zuzugreifen. In diesem Fall forderte ich Vorkehrungen, die sicherstellen, daß der Abruf bestimmter Daten nur über die dafür vorgesehenen Bildschirme möglich ist.

Generell halte ich auch programmtechnische Maßnahmen für wichtig, durch die sich der Bildschirminhalt automatisch löschen und die Zugriffsberechtigung zumindest teilweise rückgängig machen läßt, wenn eine bestimmte Zeit lang kein Abruf erfolgte. Dadurch wird der an sich zugriffsberechtigte Benutzer gezwungen, seine Abrufberechtigung erneut nachzuweisen, ein unberechtigter Benutzer jedoch daran gehindert, ohne Kenntnis der Kennwörter Daten abzurufen.

4. Teil: Neue Medien

1. Datenschutzprobleme der neuen Medien

Eine Erprobung oder Einführung der neuen Medien bringt eine Reihe datenschutzrechtlicher Gefahren mit sich; bis jetzt läßt sich deren Ausmaß nicht voll übersehen. Dies gilt vor allem für die Medien, bei denen eine selektive Auswahl aus einem beliebig großen Text- oder Bildangebot möglich ist oder bei denen eine Kommunikation zwischen Benutzern und Programmanbietern stattfindet. Bei diesen Medien ist zu erwarten, daß es zur Anlegung umfangreicher Sammlungen personenbezogener Daten in den Betriebszentralen (Bildschirmtext- oder Kabelfernseh-Zentrale) und bei den Programmanbietern kommt. Insbesondere wäre im Falle ihrer Einführung ohne Schwierigkeiten festzustellen, welcher Benutzer zu welcher Zeit welche Anbieterprogramme in welchem Umfang in Anspruch genommen hat. Aus solchen Datensammlungen läßt sich nicht nur eine Vielzahl von für sich genommen möglicherweise harmlosen Einzelinformationen gewinnen. Vielmehr könnten die Daten auch ohne Schwierigkeiten zusammengefaßt werden mit der Folge, daß umfassende Interessen- oder gar Persönlichkeitsprofile über die Benutzer erstellt werden könnten. Auch wäre es ohne weiteres denkbar, daß die entstehenden Datensammlungen über ihren ursprünglichen Zweck hinaus für eine Vielzahl anderer Zwecke verwendet werden. Sie sind vor allem für die Privatwirtschaft, die öffentliche Verwaltung (z. B. Sicherheitsbehörden) und die Politik von größtem Interesse.

2. Zielvorstellungen

Oberstes Ziel des Datenschutzes muß sein, die Erstellung von Persönlichkeitsprofilen zu verhindern. Dafür genügt es nicht, Vorkehrungen gegen den Mißbrauch gespeicherter Daten zu treffen. Vielmehr muß bereits das Erheben und Speichern personenbezogener Daten durch die Betriebszentrale und die Programmanbieter sowie das Übermitteln personenbezogener Daten zwischen diesen Stellen auf das zur Abwicklung der Dienste unbedingt erforderliche Maß reduziert werden. Auch sind personenbezogene Daten soweit irgend möglich zu anonymisieren.

Die technischen und organisatorischen Bedingungen, unter denen die einzelnen Telekommunikationsdienste zur Anwendung kommen,

sind noch nicht bekannt. Ebenso wenig ist bekannt, welche Programme im Falle einer Erprobung oder Einführung der neuen Medien tatsächlich angeboten werden. Eine abschließende datenschutzrechtliche Beurteilung ist deshalb gegenwärtig nicht möglich. Unter diesem Vorbehalt stehen meine generellen Zielvorstellungen:

- Daten der Benutzer dürfen in der Betriebszentrale nur gespeichert werden, soweit und solange dies zur Erledigung eines Dienstes unbedingt erforderlich ist.
 - Erforderlich ist eine Speicherung beispielsweise zur Abwicklung individueller Beratungsdienste, um den Informationsfluß zwischen Benutzern und Programmanbietern zu steuern.
 - Nicht erforderlich ist eine Speicherung zu Abrechnungszwecken. Die vom Benutzer zu entrichtenden Gebühren und Entgelte lassen sich wie beim herkömmlichen Fernsprechen ohne Kennzeichnung der in Anspruch genommenen Leistung erfassen. Als Abrechnungsgrundlage für die Programmanbieter genügt eine Aufstellung, welche Dienste wie häufig abgerufen wurden. Individuelle Leistungen, bei denen ohnehin personenbezogene Daten übermittelt werden, können sie jedoch selbst abrechnen.
 - Nicht erforderlich ist auch eine Speicherung von Daten der Benutzer für Zwecke der Benutzerforschung. Sie ist auf der Grundlage anonymisierter Daten möglich. Genügt dies nicht, müssen die Daten direkt bei den Benutzern erhoben werden.
- Darf die Betriebszentrale wegen der Art des in Anspruch genommenen Dienstes Daten des Benutzers an den Programmanbieter übermitteln, so muß sie den Benutzer auf die bevorstehende Datenübermittlung hinweisen. Der Benutzer hat es dann selbst in der Hand zu entscheiden, ob seine Daten übermittelt werden oder ob er von einer Inanspruchnahme des Dienstes absehen will.
- Personenbezogene Daten, die zur Steuerung des Informationsflusses zwischen Benutzer und Betriebszentrale bzw. Programmanbieter vorübergehend in der Betriebszentrale gespeichert werden müssen, sind unmittelbar nach Erledigung zu löschen.
- Den Programmanbietern ist das Erheben personenbezogener Daten, die nicht zur Erledigung des Dienstes benötigt werden, zu untersagen.
- Die Programmanbieter dürfen nach dem Grundsatz strikter Zweckbindung übermittelte Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihnen übermittelt wurden.
- Die Programmanbieter müssen alle Daten unverzüglich nach Erledigung des Dienstes löschen, es sei denn, die Speicherung erfolgt im Rahmen eines Vertrags oder vertragsähnlichen Verhältnisses zwischen Benutzer und Programmanbieter.
- Beim Rückkanal sollte festgelegt werden, in welchem Umfang und unter welchen Voraussetzungen Äußerungen von Teilnehmern dem System gegenüber abgegeben, gespeichert und übermittelt oder auf sonstige Weise genutzt werden dürfen.
- Der Datensicherung ist besondere Beachtung zu schenken. Insbesondere muß verhindert werden, daß Unbefugte etwa wegen technischer Fehlschaltungen Zugang zu den anfallenden personenbezogenen Daten erhalten.
- Eine effektive datenschutzrechtliche Kontrolle muß gewährleistet sein.

Die Zielvorstellungen lassen sich mit Hilfe des geltenden Datenschutzrechts aus folgenden Gründen nicht verwirklichen:

- Das Fernmeldegeheimnis schützt — unabhängig von seinem Geltungsbereich — nicht vor einer Speicherung personenbezogener Daten und sagt nichts über deren Löschung aus.
- Die Begriffe „Datei“ und „speichernde Stelle“ passen nicht für die neuen Medien.
- Die Einwilligung des Benutzers wird angesichts der aufgezeigten Gefahren und der Schwierigkeit einer ausreichenden Aufklärung des Benutzers in der Regel als Rechtsgrundlage für die Datenverarbeitung nicht genügen.
- Die Erlaubnistatbestände für die Datenspeicherung sind zu unbestimmt und tragen den dargestellten Gefahren nicht hinreichend Rechnung. Aus denselben Gründen muß anstelle der Sperrung nicht mehr benötigter Daten die Löschung treten.
- Die Datenerhebung wird von den Datenschutzgesetzen nicht erfaßt.
- Der Zweckbindungsgrundsatz ist in den Datenschutzgesetzen nicht strikt verwirklicht.
- Die Datenschutzgesetze gelten unter bestimmten Voraussetzungen nicht für Presse und Rundfunk (sog. Medienprivileg). Ob sich diese Regelung auch auf die neuen Medien erstreckt, bedarf angesichts der umstrittenen Einordnung der neuen Medien gesetzlicher Klärung.
- Private Programmanbieter könnten nach dem Bundesdatenschutzgesetz nur unzureichend überwacht werden. Die Datenschutzkontrolle kann derzeit nur tätig werden, wenn ein Betroffener begründet darlegt, daß er bei der Datenverarbeitung durch den Anbieter in seinen Rechten verletzt wurde. Ein Tätigwerden von Amts wegen ist nicht möglich.

Aus diesen Gründen müssen bereichsspezifische Datenschutzbestimmungen erlassen werden. Dies gilt auch für den Fall einer Erprobung der neuen Medien. Allerdings dürfen Datenschutzmaßnahmen in dieser Phase nicht dazu führen, daß potentielle Gefahren, die beim endgültigen Einsatz der neuen Medien drohen, nicht erkannt werden.

3. Möglichkeiten zur Realisierung der Zielvorstellungen

Es ist Aufgabe der Politiker zu entscheiden, ob überhaupt, zu welchem Zeitpunkt und in welchem Umfang die neuen Medien erprobt oder eingeführt werden, wer dann Träger und Betreiber der Betriebszentrale sein soll, wer als Programmanbieter in Betracht kommt und welche Grenzen bei der Programmgestaltung zu beachten sind. Solange diese Entscheidung aussteht, läßt sich nicht abschließend sagen, wie sich im konkreten Fall die Zielvorstellungen des Datenschutzes am besten verwirklichen lassen. Eine Schwierigkeit wird bei der Realisierung dieser Ziele immer die gerade im Bereich der neuen Medien mit zahlreichen Rechtsproblemen verbundene Aufteilung der Gesetzgebungskompetenz zwischen Bund und Ländern sein. Der Bundesgesetzgeber wird den Erlaß besonderer Datenschutzregelungen für den Bereich der neuen Medien frühestens erwägen, wenn an eine bundesweite Erprobung gedacht wird. Eine solche steht bislang nicht zur Diskussion. Dagegen dürfte in absehbarer Zeit der Landtag von Baden-Württemberg entscheiden, ob im Lande die neuen Medien in Form eines Pilotprojekts erprobt werden sollen oder nicht. Spricht er sich hierfür aus, ist zugleich zu bedenken, wie sich dann die Zielvorstellungen des Datenschutzes realisieren lassen. Ich bin mir wohl bewußt,

daß diese Frage nur ein allerdings bedeutsamer Aspekt der zahlreichen Problemfelder ist, die im Rahmen einer Erprobung der neuen Medien bedacht und gegeneinander abgewogen werden müssen. Hier gilt es, eine Vielzahl sich oft widerstreitender Aspekte politischer, gesellschaftlicher, wirtschaftlicher, technischer und rechtlicher Art zu gewichten und abzuwägen. Meine Aufgabe ist nur, die Belange des Datenschutzes deutlich zu machen.

Will man bei einer Erprobung neuer Medien im Lande einen effektiven Datenschutz, ließe sich das am einfachsten durch ein Landesgesetz über die Erprobung neuer Medien erreichen. Der Landesgesetzgeber hat die Kompetenz für jede notwendig erachtete Datenschutzregelung, soweit Träger und Betreiber der Betriebszentrale oder Programmanbieter einer der Aufsicht des Landes unterstehende juristische Person des öffentlichen Rechts, z. B. eine öffentlich-rechtliche Anstalt, oder eine sonstige öffentliche Stelle ist. Anders liegen die Dinge, falls die Erprobung neuer Medien mit Hilfe nicht öffentlich-rechtlicher Einrichtungen, beispielsweise einer Gesellschaft mit beschränkter Haftung oder Aktiengesellschaft als Betriebszentrale, erfolgen soll. Da der Bund den Datenschutz im privaten Bereich im Bundesdatenschutzgesetz wohl abschließend geregelt hat, könnten durch Landesgesetz wohl keine bereichsspezifischen Datenschutzvorschriften geschaffen werden. Da andererseits in der Phase der Erprobung nicht mit Regelungen auf Bundesebene zu rechnen ist, besteht die Gefahr, daß bei einer solchen Lösung die Aspekte des Datenschutzes vernachlässigt werden. Aus diesen Gründen wäre für die Erprobungsphase neuer Medien eine Lösung wünschenswert, bei der möglichst viel Datenschutz durch Landesgesetz verwirklicht werden kann.

5. Teil: Erste Erfahrungen mit dem Landesdatenschutzgesetz

Erst kurze Zeit gilt das Landesdatenschutzgesetz. Ein abschließendes Urteil, ob sich seine Regelungen bewährten, ist noch nicht möglich. Schon jetzt kann ich aber einzelne Probleme und Schwierigkeiten aufzeigen, die sich in der Praxis ergaben.

1. Anwendungsbereich des Landesdatenschutzgesetzes

1.1 Datei

Das Landesdatenschutzgesetz schützt nur personenbezogene Daten, die in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Damit kommt dem Dateibegriff zentrale Bedeutung zu. Je nachdem, wie dieser Begriff ausgelegt wird, ändert sich der Anwendungsbereich des Gesetzes. Nach der Definition in § 4 Abs. 3 LDSG ist eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen ungeordnet und ausgewertet werden kann, ungeachtet der dabei angewandten Verfahren. Wenig Schwierigkeiten bereitet die Anwendung dieser Definition im Bereich der elektronischen Datenverarbeitung, weil sie aus diesem Bereich stammt und dort eine feststehende Bedeutung hat. Anders liegt der Fall bei der nicht-automatisierten Datenverarbeitung. Hier ist vor allem problematisch, ob eine Liste als Datei anzusehen ist und wie Akten von Dateien abzugrenzen sind. Bei beiden Fragen zeigt sich mit großer Deutlichkeit, zu welcher unbefriedigenden Ergebnissen die Entscheidung des Gesetzgebers, nur die in Dateien verarbeiteten Daten unter den Schutz des Landesdatenschutzgesetzes zu stellen,

führen kann. Nach der Legaldefinition des Landesdatenschutzgesetzes kann man nicht umhin, Listen nicht als Dateien zu betrachten. Dies bedeutet z. B., daß bei einer Datenweitergabe aus einer Liste die §§ 10, 11 LDSG nicht gelten. Die Weitergabe derselben Daten aus einer Vordrucksammlung oder aus einer Kartei würde sich dagegen nach diesen Bestimmungen richten. Diese unterschiedliche Betrachtungsweise stößt vor allem bei betroffenen Bürgern auf offenes Unverständnis. Ähnlich ist die Situation bei der Datenweitergabe aus Akten. Hier kommen die großen Schwierigkeiten beim Entscheiden im Einzelfall hinzu, ob bestimmte Vorgänge noch Akten oder schon eine Datei sind. So geben letztlich manchmal Zufälligkeiten den Ausschlag, ob das Landesdatenschutzgesetz anzuwenden ist oder nicht. Die für den Gesetzgeber maßgebliche Überlegung, umordenbare Datensammlungen seien stärker mißbrauchsgefährdet und bedürften deshalb eines intensiveren Schutzes, ist im Ansatz sicherlich berechtigt. In Grenzbereichen, vor allem auf dem Gebiet der manuellen Datenverarbeitung, führt diese Regelung jedoch zu nicht befriedigenden Ergebnissen. Ich halte es deshalb für unbedingt erforderlich, dieser Frage bei einer Novellierung des Datenschutzrechts besonders aufmerksam nachzugehen. Ein erster Versuch, auf den Dateibegriff zu verzichten, findet sich in dem von der CDU/CSU-Fraktion in der letzten Legislaturperiode eingebrachten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BT-Drucksache 8/3608). Die darin gefundene Lösung wirft eine Reihe anderer Fragen auf. Diese Schwierigkeiten sollten jedoch nicht davon abhalten, weiter nach praktischen, dem Schutzbedürfnis des einzelnen Rechnung tragenden Regelungsmöglichkeiten zu suchen.

1.2 Interne Datei

Der Anwendungsbereich des Landesdatenschutzgesetzes erfährt eine weitere Einschränkung bei den internen Dateien. Dies sind Dateien mit personenbezogenen Daten, die nicht zur Übermittlung an Dritte bestimmt sind und die in nicht-automatisierten Verfahren verarbeitet werden. Für diese Dateien sind lediglich technische und organisatorische Maßnahmen der Datensicherung zu treffen. Die übrigen Bestimmungen des Landesdatenschutzgesetzes gelten nicht. Hinter dieser Regelung steckt der Gedanke, daß bei derartigen Dateien die Gefahr eines Mißbrauchs geringer ist als bei Dateien mit Daten, die weitergegeben werden. Die Verwaltungspraxis neigt, wie ich aus meinen Kontroll- und Informationsbesuchen weiß, in erheblichem Maße dazu, Karteien als interne Dateien zu bezeichnen und damit deren Daten dem Schutz des Landesdatenschutzgesetzes zu entziehen. Besonders oft geschieht dies, wenn neben den Karteien auch Akten geführt werden. In solchen Fällen machen die Behörden meist geltend, die Kartei diene lediglich der internen Arbeitserleichterung, insbesondere der Aktenerschließung. Wenn überhaupt Übermittlungen stattfänden, geschehe dies nur unter Zuhilfenahme der Akten. Bei näherer Überprüfung zeigt sich dann freilich immer wieder, daß derartige Karteien zu Unrecht als interne Dateien bezeichnet werden. Ausschlaggebend für den internen Charakter einer Datei kann nämlich nicht allein die subjektive Zweckbestimmung sein, die der Datensammlung zugemessen wird. Maßgebend kommt es auch darauf an, ob diese Zweckbestimmung tatsächlich eingehalten werden kann und eingehalten wird. Daß die Beantwortung dieser Frage in Einzelfällen Schwierigkeiten bereiten kann, liegt auf der Hand. Gleichwohl hängt davon in vielen Fällen die Anwendbarkeit des Landesdatenschutzgesetzes ab. Auch hier stellt sich die Frage, ob dies sachgerecht ist und ob

nicht geeigneterer, leichter feststellbare Kriterien für die Anwendbarkeit des Landesdatenschutzgesetzes gefunden werden können.

1.3 Beschränkung auf Datenverarbeitung ohne Datenerhebung

Personenbezogene Daten fallen im Grundsatz nur unter den Schutz des Landesdatenschutzgesetzes, soweit eine Datenverarbeitung stattfindet. Dieser Begriff ist in § 1 Abs. 1 LDSG näher definiert. Zur Datenverarbeitung zählt danach zwar das Speichern von Daten, das heißt das Erfassen, Aufnehmen oder Auf sammeln von Daten auf einen Datenträger zum Zwecke der weiteren Verwendung, nicht aber das Beschaffen, Ermitteln, Recherchieren und Einsammeln von Daten. Diese Unterscheidung ist ohne wesentliche Auswirkungen, wenn beide Vorgänge in einem Zuge erfolgen, wenn also Erhebung und Speicherung zusammenfallen. Dies ist aber keineswegs stets der Fall. Immer wieder kommt vor, daß zwar Daten erhoben, diese aber anschließend nicht in einer Datei gespeichert werden. Die Behörde wertet sie zunächst aus und speichert erst das Ergebnis der Auswertung in einer Datei. Ein Beispiel mag dies verdeutlichen. In einer Eingabe beschwerte sich ein Beamtenanwärter darüber, bei seinem Eintritt in den Vorbereitungsdienst sei er in einem Vordruck aufgefordert worden, den Arbeitgeber seiner Ehefrau anzugeben. Das Landesamt für Besoldung und Versorgung und das Finanzministerium teilten mir auf Anfrage mit, diese Angabe würde zur Berechnung der Höhe des Verheiratetenzuschlags benötigt. Denn nach den besoldungsrechtlichen Bestimmungen sei die Höhe dieses Zuschlags u. a. davon abhängig, ob der Ehegatte im öffentlichen Dienst oder einer ihm gleichgestellten Tätigkeit beschäftigt sei. Die Entscheidung über das Vorliegen dieser Voraussetzung könne nicht dem einzelnen Beamten überlassen bleiben, da diese Begriffe äußerst komplex seien und selbst erfahrene Sachbearbeiter mitunter Schwierigkeiten hätten. Aus diesem Grunde müsse der jeweilige Arbeitgeber angegeben werden. Auf der Grundlage dieser Angaben könne dann das Landesamt für Besoldung und Versorgung entscheiden, ob der Ehegatte im öffentlichen Dienst oder einer ihm gleichgestellten Tätigkeit beschäftigt ist. Nur dieses aus den Angaben des Beamten gewonnene Datum wurde anschließend in einer Datei gespeichert. Fälle dieser Art werden weder vom Landesdatenschutzgesetz noch vom Bundesdatenschutzgesetz erfaßt. Beide Gesetze regeln eine derartige Datenerhebung nicht. Ich halte diese Ausklammerung der Datenerhebung aus dem Anwendungsbereich der Datenschutzgesetze für problematisch. Durch den Datenschutz soll der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegengewirkt werden. Eine derartige Beeinträchtigung kann aber bereits bei der Datenerhebung eintreten. Ich halte für notwendig, bereits bei der Erhebung der Daten mit dem Datenschutz einzusetzen und auf diese Weise das Ansammeln von Daten zu begrenzen.

2. Datengeheimnis

Die Regelung des § 7 LDSG über die Verpflichtung auf das Datengeheimnis bereitet in der Praxis erhebliche Schwierigkeiten. Schuld daran ist vor allem die unbestimmte Umschreibung des Personenkreises, der zu verpflichten ist. Insbesondere im Bereich der manuellen Datenverarbeitung herrscht erhebliche Unklarheit. So verpflichten viele Stellen gewissermaßen auf Verdacht alle Bediensteten, die in irgendeiner Form mit personenbezogenen Daten in Berührung kommen können. Verschiedene Behörden gingen sogar so weit, alle

Bediensteten einschließlich der Reinigungskräfte auf das Datengeheimnis zu verpflichten. Ich halte diese Praxis für bedenklich. Solche Verpflichtungen entwerten das Datengeheimnis und schmälern seine Bedeutung. Das angewandte Verfahren verstärkt meine Bedenken noch. Denn zumeist erhielten die Bediensteten einen Vordruck zur Unterschrift vorgelegt, in dem der Wortlaut des § 7 Abs. 1 LDSG in etwa wiedergegeben war und zusätzlich noch auf mögliche strafrechtliche und disziplinarrechtliche Konsequenzen hingewiesen wurde. Nicht erläuterte man ihnen, was das Datengeheimnis beinhaltet und was Sinn und Zweck der Verpflichtung ist. Ebenso unterblieb jede Erklärung, wie sich das Datengeheimnis zur allgemeinen Verschwiegenheitspflicht nach Beamten- und Tarifrecht verhält. Diese Verfahrensweise rief den Eindruck hervor, bei der Verpflichtung auf das Datengeheimnis handle es sich um einen reinen Formalakt. Ich habe deshalb Verständnis für die zahlreichen Anrufe und Schreiben, insbesondere aus Kreisen der Lehrerschaft, die auf die Fragwürdigkeit einer derartigen Verpflichtungspraxis hinwiesen. Führt man eine Verpflichtung auf das Datengeheimnis in der geschilderten Weise durch, wird man zwar formal dem Gesetz genüge tun. Eine Stärkung des Datenschutzgedankens ist dies aber sicher nicht, im Gegenteil: der dabei entstehende bürokratische Verwaltungsaufwand führt zu Aversionen gegenüber dem Datenschutz, der Begriff Datenschutz wird gleichgestellt mit dem Begriff Bürokratie. Durch die Verpflichtung auf das Datengeheimnis soll den bei der Datenverarbeitung beschäftigten Personen ihre Pflicht zur Wahrung des Datengeheimnisses in besonders augenfälliger Weise deutlich gemacht werden. Dieses vom Gesetzgeber beabsichtigte Ziel läßt sich nur dann erreichen, wenn der einzelne Bedienstete über Bedeutung und Gegenstand des Datengeheimnisses sowie über Sinn und Zweck der Verpflichtung umfassend informiert und dabei möglichst auch auf die Auswirkungen des Datengeheimnisses auf seine konkrete Tätigkeit hingewiesen wird. Eine formelhafte Wiedergabe des Gesetzestextes erfüllt diese Anforderungen nicht. Ohne eine solche umfassende Belehrung halte ich eine Verpflichtung auf das Datengeheimnis sogar für schädlich. Sollte eine Verbesserung der Verpflichtungspraxis nicht möglich sein, dann wäre zu überlegen, ob nicht den Interessen des Datenschutzes besser gedient wäre, wenn man von einer Verpflichtung auf das Datengeheimnis generell absehen würde.

3. Hinweispflicht

Das Landesdatenschutzgesetz will den informierten Bürger. Deshalb müssen nach § 9 Abs. 2 LDSG die Behörden jeden Bürger, bei dem sie Daten zu Speicherungszwecken erheben, über die rechtliche Grundlage ihrer Datenerhebung aufklären. Muß der betroffene Bürger Angaben machen, ist die Rechtsvorschrift anzugeben, aus der sich diese Verpflichtung ergibt. Besteht keine Rechtspflicht zur Angabe, muß die Behörde den Bürger auf die Freiwilligkeit seiner Angabe hinweisen. Bedauerlicherweise fand diese Regelung bislang in die Verwaltungspraxis noch wenig Eingang. Zum Teil liegt dies daran, daß viele Vordrucke noch nicht der neuen Rechtslage angepaßt sind. Zu einem wesentlichen Teil führe ich diese Anpassungsschwierigkeiten jedoch auf die geringe Aufmerksamkeit zurück, die man in der Vergangenheit der Datenerhebung schenkte. Grund dafür ist wiederum der Umstand, daß weite Bereiche das Erheben von personenbezogenen Daten noch nicht als Eingriff in die Rechtsstellung des Bürgers ansehen. Davon ließ sich ganz offensichtlich auch der Gesetzgeber leiten. So legte er häufig in Rechtsvorschriften nicht im einzelnen fest, welche personenbezogenen Daten anzugeben sind. Folglich fehlen vielfach einzelne konkrete Bestimmungen, an denen sich eine Verpflichtung zur Angabe persönlicher Daten ergibt. An zwei

Beispielen möchte ich dies verdeutlichen. Weder das Schulgesetz noch eine auf der Grundlage dieses Gesetzes ergangene Rechtsverordnung geben an, welche Daten des Schülers und der Erziehungsberechtigten bei Anmeldung eines schulpflichtigen Kindes angegeben werden müssen. § 115 des Schulgesetzes legt eine Auskunftspflicht nur für den Fall der Durchführung statistischer Erhebungen fest. Dasselbe gilt für den Hochschulbereich. Auch hier ist im einzelnen nicht geregelt, welche Angaben ein Student bei der Immatrikulation machen muß. In diesen Fällen läßt sich allenfalls mittelbar aus dem Gesamtzusammenhang der gesetzlichen Regelung schließen, zu welchen Angaben die Studenten verpflichtet sind. Es liegt auf der Hand, daß unter diesen Umständen die Erfüllung der Hinweispflicht nach § 9 Abs. 2 LDSG den betroffenen Stellen erhebliche Schwierigkeiten bereitet. Ich halte es deshalb für unerlässlich, daß in Zukunft beim Erlaß von Rechtsvorschriften dieser Frage besondere Aufmerksamkeit geschenkt und jeweils klargestellt wird, inwieweit eine Auskunftspflicht besteht.

Schwierigkeiten bereitet die Regelung des § 9 Abs. 2 LDSG auch dann, wenn eine Behörde auf Antrag tätig werden soll. Im Regelfall ist hier ebenfalls nicht in einer Rechtsvorschrift konkret bestimmt, welche persönlichen Daten der Antragsteller angeben muß. Andererseits kann man aber auch nicht davon sprechen, die Angaben seien freiwillig. In diesen Fällen kommt die Behörde ihrer Aufklärungspflicht nach § 9 Abs. 2 LDSG am ehesten durch einen Hinweis an den Antragsteller nach, eine positive Entscheidung seines Antrags sei nur dann möglich, wenn er im einzelnen näher bezeichnete Daten angibt. Ebenso sollten die Behörden verfahren, wenn im Zusammenhang mit dem Abschluß eines Vertrags Daten erhoben werden. Auch hier empfiehlt sich, dem Vertragswilligen zu sagen, ein Vertragsabschluß sei nur bei Angabe bestimmter Daten möglich.

Die Hinweispflicht nach § 9 Abs. 2 LDSG ist letztlich Ausfluß des Prinzips des sozialen Rechtsstaats. Dieses Prinzip verlangt von der Verwaltung, nicht nur die Rechte des Bürgers zu achten sondern ihn darüber auch umfassend zu informieren. Nicht zuletzt aus diesem Grund vertreten manche die Auffassung, die Hinweispflicht gelte für jede Art der Erhebung personenbezogener Daten. Sie sei unabhängig davon, ob die Daten in einer Datei oder in sonstiger Weise gespeichert werden. Diese strittige Rechtsfrage sollte in der Verwaltungspraxis keine entscheidende Rolle spielen. Denn für eine Verwaltung, die sich der Bürgerfreundlichkeit verpflichtet weiß, sollte es eine Selbstverständlichkeit sein, den Bürger auf die Rechtsgrundlage hinzuweisen, wenn sie von ihm Daten verlangt.

4. Datenübermittlung

Die Frage, ob und unter welchen Voraussetzungen eine öffentliche Stelle von ihr gespeicherte Daten an eine andere Stelle weitergeben darf, ist eine der wichtigsten des Datenschutzrechts überhaupt. Deshalb kommt der Beachtung der Vorschriften über die Datenübermittlung eine besondere Bedeutung zu. Wie kaum anders zu erwarten war, herrscht in diesem Bereich zur Zeit noch erhebliche Unsicherheit. Teils wird nahezu jede Übermittlung abgelehnt; teils wird noch so verfahren, als ob es eine Datenschutzgesetzgebung überhaupt nicht gäbe. Gerade hier zeigen sich besonders deutlich die Probleme, die eine sehr allgemein gehaltene, mit unbestimmten Begriffen arbeitende Gesetzgebung in der Praxis aufwirft. Gesetzesbegriffe wie „Beeinträchtigung schutzwürdiger Belange“, „berechtigtes Interesse“ und „zur rechtmäßigen Erfüllung der Aufgaben erforderlich“ laden geradezu zu unterschiedlichen Interpretationen ein. Dies ist sicherlich ein Zustand, der auf Dauer nicht befriedigen kann. Ich hoffe jedoch, daß im Laufe der Zeit für die einzelnen Sachgebiete einheit-

liche Maßstäbe entwickelt werden und daß auf diese Weise eine einheitliche Verwaltungspraxis sichergestellt wird. Auf die Entwicklung derartiger Maßstäbe hinzuwirken, ist eine meiner Aufgaben im Rahmen meiner Aufsichts- und Beratungstätigkeit. Zur Anwendungspraxis der Übermittlungsvorschriften sind folgende Gesichtspunkte wichtig:

- Das Landesdatenschutzgesetz verpflichtet eine speichernde Stelle nicht, Daten zu übermitteln. Es legt lediglich die Voraussetzungen fest, unter denen sie übermittelt werden dürfen.
- Die Verwaltung ist datenschutzrechtlich keine Einheit. Das Landesdatenschutzgesetz ordnet die Daten vielmehr jeweils den einzelnen Behörden zu, welche die Daten speichern. Sie hat im Regelfall jeweils darüber zu entscheiden, ob Daten weitergegeben werden dürfen oder nicht.
- Bei Datenübermittlungen an private Stellen besteht eine gewisse Scheu, die Einwilligung der Betroffenen einzuholen. Diese Zurückhaltung sollte aufgegeben werden und die Entscheidung, ob Daten weitergegeben werden sollen, der autonomen Entscheidung des Bürgers überlassen bleiben. Die Befürchtung, dann würden aus Gleichgültigkeit wünschenswerte Datenübermittlungen unterbleiben, teile ich nicht. Sie geht vom Bild eines Bürgers aus, der nicht in der Lage und nicht bereit ist, berechnete Anliegen zu prüfen und daraus Konsequenzen zu ziehen. Diese pessimistische Grundhaltung kann ich nicht teilen. Man kann vom mündigen Bürger nicht nur reden, man muß ihn auch als solchen behandeln.

5. Datenverarbeitung im Auftrag

Datenverarbeitung erfolgt entweder durch die Behörde, die die Daten speichert, selbst oder aber durch eine von ihr beauftragte Person oder Stelle. In letzterem Fall wird der Datenaustausch zwischen Auftraggeber und Auftragnehmer nicht als Datenübermittlung betrachtet mit der Folge, daß insoweit auch nicht die Übermittlungsvorschriften des Landesdatenschutzgesetzes anzuwenden sind. Der Auftraggeber bleibt Herr der Daten. Speichern, Übermitteln, Verändern und Löschen personenbezogener Daten ist nur im Rahmen seiner Weisungen zulässig. Er ist für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Deshalb muß er den Auftragnehmer sorgfältig auswählen und sich Kontrollmöglichkeiten vorbehalten.

Eine derartige Datenverarbeitung im Auftrag erfolgt vor allem im Bereich der automatisierten Datenverarbeitung. So wickeln die Regionalen Rechenzentren für die Kommunen des Landes eine Vielzahl von Verfahren ab, die die Verarbeitung personenbezogener Daten zum Gegenstand haben. Aber auch im staatlichen Bereich betreiben Rechenzentren Auftragsdatenverarbeitung für Behörden und sonstige öffentliche Stellen. Private Auftragnehmer werden vor allem bei der Datenerfassung eingesetzt.

Bei Kontrollbesuchen stellte ich vielfach fest, daß sich die auftraggebenden Behörden nicht immer der Tatsache bewußt sind, daß sie auch bei der Beauftragung eines Rechenzentrums uneingeschränkt für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich sind. Insbesondere sind sich diese Behörden nicht immer im erforderlichen Maße darüber im klaren, daß die Datenverarbeitung nach ihrer Weisung zu erfolgen hat und sie auch kontrollieren müssen, ob die Auftraggeber die datenschutzrechtlichen Bestimmungen einhalten. Zu dieser Verkennung der Verantwortlichkeit trägt im staatlichen Bereich sicher das Nebeneinander von Auftrags- und Weisungsverhältnis bei. Dies wird besonders in den Fällen deutlich, wo, wie etwa im Bereich der Finanzverwaltung, die Oberfinanz-

direktion, also die übergeordnete, weisungsberechtigte Behörde zugleich auftragnehmende Stelle des Finanzamts, also der nachgeordneten, weisungsgebundenen Behörde, ist. Gleichwohl meine ich, daß auch in solchen Fällen im Interesse der Sicherstellung der Verantwortlichkeit Klarheit über das Auftragsverhältnis und die sich daraus ergebenden Rechte und Pflichten bestehen muß.

Immer wieder steht auch die Frage zur Diskussion, unter welchen Voraussetzungen überhaupt von einer Datenverarbeitung im Auftrag ausgegangen werden kann. Problematisch ist dies, wenn eine Behörde eine andere Stelle mit der Wahrnehmung bestimmter Aufgaben beauftragt und dabei eine Datenverarbeitung stattfindet. So wollte man von mir wissen, ob das Durchführen einer statistischen Untersuchung durch eine andere Stelle als Datenverarbeitung im Auftrag anzusehen ist und demzufolge die Weitergabe der für die Untersuchung erforderlichen Daten an die beauftragte Stelle keiner Beschränkung unterliegt. Ich verneinte diese Frage, weil es sich um Datenverarbeitung im Auftrag nur dann handelt, wenn sich der Auftrag auf die technische Durchführung der Datenverarbeitung beschränkt. In dem geschilderten Beispiel war dies gerade nicht der Fall; hier wurde nicht nur die technische Abwicklung, sondern die gesamte Aufgabe „Durchführung der statistischen Untersuchung“ übertragen. Die beauftragte Stelle verarbeitete daher die Daten für ihre eigene Aufgabe, eine statistische Untersuchung vorzunehmen, und nicht für die andere Behörde, die dazu den Auftrag erteilte.

6. Sperrung und Löschung

Sperrung und Löschung sind wichtige Maßnahmen zur Sicherstellung des Datenschutzes. Unter den Voraussetzungen der §§ 6 und 13 LDSG hat der Bürger ein Recht darauf, daß seine Daten gesperrt oder gelöscht werden. Leider wendet die Praxis diese für den Datenschutz wesentlichen Regelungen noch nicht in vollem Umfang an. So zeigte sich bei Kontrollbesuchen, daß automatisierte Verfahren vielfach überhaupt keine Möglichkeit zur Sperrung sei es aller, sei es bestimmter Datenarten vorsehen. Zur Begründung tragen die Behörden dann vor, dazu habe vor Erlaß des Landesdatenschutzgesetzes kein Anlaß bestanden. Dies mag eine Erklärung sein, ändert aber nichts daran, daß das Landesdatenschutzgesetz eine Sperrung kennt und folglich überall dort eine Sperrmöglichkeit vorgesehen werden muß, wo ein Bedürfnis für eine Sperrung auftreten kann. In einem Fall mußte ich sogar feststellen, daß eine Behörde dem Verlangen des Betroffenen nach Löschung nicht entsprechen konnte, obwohl sie die Daten von Anfang an unzulässig speicherte und deshalb hätte löschen müssen. Eine Nachprüfung ergab, daß das dort eingesetzte EDV-Verfahren eine Löschmöglichkeit nicht kennt. Ich beanstandete diesen offensichtlichen Verstoß gegen § 13 LDSG und forderte die Behörde auf, umgehend eine Löschmöglichkeit zu schaffen. Zwar handelt es sich beim Fehlen einer Löschmöglichkeit sicher um Einzelfälle. Aber auch, wenn automatisierte Verfahren eine Löschmöglichkeit vorsehen, unterbleibt häufig die Löschung nicht mehr benötigter Daten von Amts wegen. Ein wesentlicher Grund dafür ist die Schwierigkeit, im Einzelfall zu entscheiden, wann die Löschungsvoraussetzungen vorliegen. Bei manueller Datenverarbeitung kommt der erhebliche Verwaltungsaufwand hinzu, den eine Löschung vor allem bei umfangreichen Dateien verursacht. Dieser Umstand trägt nicht dazu bei, die Bereitschaft zu erhöhen, Löschungen nicht nur vorzunehmen, wenn dazu eine Verpflichtung besteht, sondern schon dann, wenn die Löschungsvoraussetzungen gegeben sind. Ungeachtet dieser nicht zu leugnenden Probleme halte ich es für unerlässlich, daß von der Löschmöglichkeit wesentlich mehr als bisher Gebrauch gemacht wird. Nur auf diese Weise läßt

sich eine nur sehr schwer zu kontrollierende Dauerspeicherung von Daten verhindern. Dieses Ziel ließe sich in vielen Fällen durch das Einführen regelmäßiger Lösungsfristen erreichen. Sie würden dazu zwingen, die Notwendigkeit der Speicherung im Einzelfall zu überprüfen.

7. Verwaltungsvorschriften

Das Landesdatenschutzgesetz regelt den Datenschutz einheitlich für sämtliche Bereiche der öffentlichen Verwaltung des Landes. Dieser umfassende Anwendungsbereich führte zu einem hohen Abstraktionsgrad der einzelnen Regelungen, da Rechtsvorschriften geschaffen werden mußten, die auf alle Bereiche Anwendung finden können. Dies war nur durch die Verwendung zahlreicher unbestimmter Gesetzesbegriffe möglich. Eine derartige Gesetzgebungstechnik eröffnet sowohl Gefahren als auch Chancen. Die Gefahren sehe ich darin, daß diese unbestimmten Gesetzesbegriffe zu sehr unterschiedlichen Interpretationen und damit zu einer unterschiedlichen Verwaltungspraxis führen. Als Chance betrachte ich, daß diese Regelungen dank ihrer Elastizität den Besonderheiten der einzelnen Verwaltungsbereiche Rechnung tragen und dabei gleichwohl die Einheitlichkeit des Datenschutzes im Grundsatz wahren. Ein wichtiges Hilfsmittel dazu könnte der Erlaß von Verwaltungsvorschriften sein. Wünschenswert sind nicht so sehr Verwaltungsvorschriften, die allgemein die Ausführung des Landesdatenschutzgesetzes näher regeln. Für dringlicher und für die Verwaltungspraxis sicherlich hilfreicher hielte ich Hinweise über die Auswirkungen des Landesdatenschutzgesetzes auf einzelne Verwaltungsbereiche, in denen dafür ein besonderes Bedürfnis besteht. Nach meiner bisherigen Erfahrung denke ich dabei insbesondere an den Schulbereich und an die Gesundheitsverwaltung.

8. Wissenschaftliche Forschung

Die wissenschaftliche Forschung empfindet den Datenschutz vielfach als nicht gerechtfertigten Hemmschuh. Durch ihn fühlt sie sich in ihrer durch die Verfassung garantierten Unabhängigkeit beeinträchtigt. In der Tat läßt sich nicht leugnen, daß der Datenschutz gerade in diesem Bereich Probleme aufwirft. Letztlich geht es hier um die Notwendigkeit, einen angemessenen Ausgleich zwischen dem Persönlichkeitsrecht des einzelnen und der Wissenschaftsfreiheit zu finden. Das Landesdatenschutzgesetz nahm sich in § 20 dieser Problematik an und versuchte, dieses Spannungsverhältnis zu regeln. Meine bisherige Tätigkeit läßt naturgemäß noch kein abschließendes Urteil darüber zu, wieweit sich diese Regelung bewährte. Schon jetzt zeigten sich jedoch verschiedene Punkte, die der Diskussion bedürfen.

Problematisch ist einmal, daß § 20 LDSG nur auf Hochschulen und andere öffentlichen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung Anwendung findet. Bei verschiedenen Universitäten des Landes bestehen privatrechtlich organisierte Einrichtungen, die eng mit der Universität verflochten sind. Diese Einrichtungen führen vielfach Forschungsvorhaben für die Universitäten durch, da diese selbst nicht immer über die erforderlichen sachlichen und personellen Mittel verfügen. Meist wird die Einrichtung auch mit öffentlichen Mitteln finanziert. Selbst wenn eine so enge Verflechtung gegeben ist, muß nach der gegenwärtigen Rechtslage eine derartige Einrichtung in datenschutzrechtlicher Hinsicht behandelt werden wie eine ganz normale juristische Person des Privatrechts. Dies führt vor allem dann zu Schwierigkeiten, wenn eine Hochschule sie mit der Durchführung von Forschungsvorhaben beauftragt.

In diesen Fällen kann die Hochschule von ihr zu Forschungszwecken gespeicherte Daten nach § 20 Abs. 2 LDSG nur mit Einwilligung des Betroffenen an die Institution weitergeben, während andere öffentliche Stellen dies unter den Voraussetzungen des § 11 LDSG auch ohne Einwilligung tun können.

Vor erhebliche Probleme sieht sich die zeitgeschichtliche Forschung dadurch gestellt, daß § 20 Abs. 3 LDSG eine Veröffentlichung von Forschungsergebnissen, soweit sie personenbezogene Daten enthalten, nur mit Einwilligung des Betroffenen zuläßt. Da eine solche Einwilligung in vielen Fällen gar nicht eingeholt werden kann, ist es beim derzeitigen Gesetzeswortlaut weitgehend unmöglich, ohne Verstoß gegen das Landesdatenschutzgesetz in wissenschaftlichen Veröffentlichungen personenbezogene Daten von Personen der neueren Geschichte anzuführen. Dies gilt selbst für solche Daten, die als allgemein zugängliche Quellen entnommen und der Öffentlichkeit weitgehend bekannt sind. § 20 Abs. 3 LDSG ist insoweit noch wesentlich restriktiver als die allgemeinen Übermittlungsregelungen des Landesdatenschutzgesetzes, ohne daß dafür ein zwingender Grund ersichtlich wäre.

Ein besonderes Problem stellt sich für die medizinische, insbesondere die epidemiologische Forschung. In diesem Bereich ist bei der Weitergabe von Daten neben den Übermittlungsregelungen der Datenschutzgesetze auch die ärztliche Schweigepflicht zu beachten. Die der Schweigepflicht unterliegenden Tatsachen und Befunde dürfen auch für Forschungszwecke nur soweit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt (vgl. § 2 Abs. 7 der Berufsordnung der Landesärztekammer Baden-Württemberg). Entgegen einer immer wieder vorgetragenen, in der Vergangenheit auch praktizierten Auffassung ist diese Anonymität nicht schon dann gesichert, wenn bei der Weitergabe medizinischer Daten lediglich der Name des Patienten nicht mitgeteilt, dagegen aber eine ganze Reihe anderer Daten übermittelt werden, die eine Identifizierung des Patienten ohne größere Schwierigkeiten zulassen. Ich bin mir durchaus bewußt, daß gerade die Frage der Weitergabe medizinischer Daten zu Forschungszwecken kontrovers diskutiert wird. Bei der derzeitigen Gesetzeslage muß ich jedoch davon ausgehen, daß nicht anonymisierte medizinische Daten ohne Zustimmung des betroffenen Patienten nicht für Forschungszwecke übermittelt werden dürfen. Angesichts der Sensibilität, die gerade medizinischen Daten zukommt, und der Schutzbedürftigkeit des Arzt/Patienten-Verhältnisses halte ich dieses Ergebnis für richtig. Hält man gleichwohl die Weitergabe medizinischer Daten zu bestimmten Forschungszwecken für unbedingt geboten, dann bedarf es dazu einer Entscheidung des Gesetzgebers.

6. Teil: Fortentwicklung des Datenschutzrechts

1. Novellierung des Bundesdatenschutzgesetzes

Mit dem Erlaß des Bundesdatenschutzgesetzes wurde der Versuch unternommen, den Datenschutz umfassend für alle Bereiche zu regeln. Bei einer derartigen Konzeption konnte es nicht ausbleiben, daß schon bald nach Inkrafttreten des Gesetzes der Ruf nach einer Novellierung laut wurde. Die Befürworter forderten vor allem eine

- Präzisierung der zahlreichen unbestimmten Gesetzesbegriffe
- Aufgabe des Dateibegriffs
- Ausdehnung des Anwendungsbereichs auf die Datenerhebung und jede Art der Datennutzung

- stärkere Zweckbindung der Daten
- Konkretisierung der Datensicherungsvorschriften
- Gebührenfreiheit für die Erhebung von Auskünften
- Verbesserung der Rechtstellung der betrieblichen Datenschutzbeauftragten
- Ausdehnung der Kontrollbefugnis der Aufsichtsbehörde
- Einräumung eines verschuldensunabhängigen Schadensersatzanspruchs.

Ein erster Versuch zu einer Novellierung des Bundesdatenschutzgesetzes blieb in der letzten Legislaturperiode des Deutschen Bundestags ohne Erfolg. Nach den Ankündigungen der Bundesregierung und der im Bundestag vertretenen Parteien ist zu erwarten, daß sich der neue Bundestag erneut mit der Frage einer Novellierung des Bundesdatenschutzgesetzes befaßt. Da eine derartige Gesetzesänderung zugleich Auswirkungen auf das Landesdatenschutzgesetz hätte, messe ich diesen Bemühungen auch für meine Tätigkeit große Bedeutung zu.

Die bisherige Diskussion über die Novellierung des Bundesdatenschutzgesetzes zeigte deutlich, daß es zwar verhältnismäßig leicht fällt, die Schwächen einzelner Regelungen aufzuzeigen, daß es aber sehr viel schwerer ist, bessere Vorschläge zu machen. Deshalb sollte eine Novellierung sehr sorgfältig vorbereitet werden. Dazu ist es notwendig, die bisherigen Erfahrungen mit den Datenschutzgesetzen auszuwerten und die Auswirkungen möglicher Änderungen eingehend zu analysieren. Dies kann sicherlich nicht kurzfristig geschehen. Zu einer besonderen Eile besteht aber auch kein Anlaß. Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sind zwar durchaus verbesserungsbedürftig und verbesserungsfähig; die bestehenden Mängel sind jedoch nicht so, daß eine sofortige Gesetzesänderung unbedingt geboten wäre.

2. Bereichsspezifische Regelungen

2.1 Bedürfnis

Sowohl das Bundesdatenschutzgesetz als auch das Landesdatenschutzgesetz sind als Auffanggesetze angelegt. Sie beanspruchen Geltung nur insoweit, als der Datenschutz nicht in einer speziellen, den Besonderheiten eines bestimmten Bereichs Rechnung tragenden Rechtsvorschrift geregelt ist. Es besteht weitgehend Einigkeit darüber, daß derartige bereichsspezifische Regelungen unverzichtbar sind und daß auch noch nach dem Erlaß des Melde-rechtsrahmengesetzes, des Personalausweisgesetzes und der Novellierung des Sozialheimnisses im Sozialgesetzbuch ein Bedürfnis für die Schaffung weiterer Regelungen besteht. Auch künftig wird es notwendig werden, Besonderheiten einzelner Sachgebiete durch besondere Datenschutzbestimmungen Rechnung zu tragen.

2.2 Gefahren

Diese Tendenz zum bereichsspezifischen Datenschutz birgt jedoch auch gewisse Gefahren in sich. So darf es nicht geschehen, daß gleiche Sachverhalte in unterschiedlichen Rechtsgebieten ungleich behandelt werden. Damit würde die unbedingt notwendige Einheitlichkeit aufgegeben, der Datenschutz gewissermaßen atomisiert werden. Jede Übersicht ginge verloren und das große Verdienst der allgemeinen Datenschutzgesetze, zu der Entwicklung eines umfassenden Datenschutzbegriffs beigetragen zu haben, würde aufgegeben. Eine weitere Gefahr darf nicht über-

sehen werden. Die Schaffung bereichsspezifischer Regelungen gibt Interessengruppen leichter die Chance, ihre Ziele durchzusetzen. Das kann zu einer Verwässerung des Datenschutzes führen.

2.3 Forderung

Aus diesen Gründen halte ich es für geboten, die Notwendigkeit bereichsspezifischer Regelungen im Einzelfall sehr sorgfältig zu prüfen. Bereichsspezifischer Datenschutz ist kein Wert an sich. Zu dieser Lösung sollte nur dort gegriffen werden, wo dies unumgänglich notwendig ist. In jedem Fall sollte aber darauf geachtet werden, daß die Einheitlichkeit des Datenschutzes sichergestellt bleibt. Dazu gehört es beispielsweise auch, für gleiche Sachverhalte nach Möglichkeit dieselben Gesetzesbegriffe zu verwenden. Bevor an den Erlaß von Rechtsvorschriften herangegangen wird, ist darüber hinaus zu überlegen, ob sich das angestrebte Ziel nicht durch den Erlaß von Verwaltungsvorschriften erreichen läßt. Derartige Verwaltungsvorschriften können insbesondere für eine einheitliche Verwaltungspraxis sorgen und damit eine sich aus unterschiedlichen Interpretationen ergebende Rechtsunsicherheit beseitigen. Gerade dies ist aber häufig Anlaß dazu, den Erlaß bereichsspezifischer Rechtsvorschriften zu verlangen.

Schlußbemerkung

Dieser Tätigkeitsbericht kann und will kein umfassendes Bild über die Situation des Datenschutzes in Baden-Württemberg geben. Allein der Versuch dazu wäre vermessen, da ich erst kurze Zeit mein Amt ausübe. Der Bericht ist auch keine abschließende Aufzählung meiner Aktivitäten. Er beschränkt sich bewußt auf Schwerpunkte. Mir kam es vor allem darauf an zu informieren, wie ich mein Amt verstehe, welche Ziele ich verfolge und welche Methoden ich anwende. Wichtig erschien mir auch darzustellen, wie die Verwaltung auf das Landesdatenschutzgesetz und mein Amt reagierte und welche generellen Probleme und Schwierigkeiten der Datenschutz in der Praxis aufwirft.