9. Wahlperiode

zu Drucksache **9/5873**

HESSISCHER LANDTAG

15. 01. 82

Zehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 15. Januar 1982 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 15. Januar 1982 - Ausgegeben am 19. Februar 1982

Druck und Auslieferung: Kanzlei des Hessischen Landtags - Postfach 32 40 - 6200 Wiesbaden 1

INHALTSVERZEICHNIS

Seite

1. ZUR SITUATION ... 5
2. BILANZ ... 8
2.1 Zum 7. Tätigkeitsbericht für 1978 (Drucks. 9/67) ... 8
2.1.1 Vorsorgeuntersuchung bei der Einschulung ... 8
2.2 Zum 8. Tätigkeitsbericht für 1979 (Drucks. 9/2740) ... 9
2.2.1 Wissenschaftliche Forschung und Datenschutz ... 9
2.2.2 Kriminalpolizeiliche Sammlungen ... 9
2.3 Zum 9. Tätigkeitsbericht für 1980 (Drucks. 9/4032) ... 9
2.3.1 Direktverbindung zwischen Polizei und Kfz.-Zulassungstelle ... 9
2.3.2 Neuregelung des Datenschutzes im Hessischen Krankenhausgesetz ... 10
2.3.3 Krebsregister ... 10
2.3.4 Datenverarbeitung durch den Verfassungsschutz ... 10
2.3.5 Das Melderechtsrahmengesetz und die Novellierung des Landesmelderechts ... 11
2.3.6 Datenschutz im Hochschulbereich ... 11
2.3.7 Datensicherung - Forderungen an Automationsvorhaben der Verwaltung ... 11
3. AUFGABEN ... 12
3.1 Novellierung des Bundesdatenschutzgesetzes ... 12
3.2 Archivgesetz ... 20
3.3 "Verrechtlichung" der Verarbeitung personenbezogener Daten durch die Polizei ... 24
3.4 Krebsregister-Gesetz ... 25
4. DATENSCHUTZPROBLEME - ERFAHRUNGEN UND BEISPIELE ... 27
4.1 Datenschutz im Sozialbereich ... 27
4.2 Geheimhaltung und innerbehördliche Kommunikationsschranken ... 33
4.3 Datenaustausch innerhalb der Gemeinde: Informationseinheit oder Übermittlungsschranken? ... 38
4.4 Praxis der Datenschutzkontrolle ... 39
4.5 Exemplarische Einzelfälle ... 45
4.5.1 Masseneinwendungen im atomrechtlichen Genehmigungsverfahren ... 45
4.5.2 Kontrollmitteilungen an die Finanzämter ... 46
4.5.3 Übermittlung der Daten von Krankenhauspatienten an die Polizei ... 47
4.5.4 Amtshilfe im Ermittlungsverfahren und Schutz des Betroffenen ... 47
4.5.5 Regelmäßige Auswertung von Meldescheinen durch die Polizei ... 48
4.5.6 Begleituntersuchung zum Test für medizinische Studiengänge ... 49
4.5.7 Übermittlung der Daten von Religionslehrern an die Kirchen ... 50
4.5.8 Offenbarung von Sozialdaten an Kreditinstitute ... 52

5. MATERIALIEN 54

5.1 Erlaß des Hessischen Ministers des Innern vom 13.6.1981 (StAnz. S. 1262) betr. die Übermittlung von personenbezogenen Daten an öffentliche Forschungseinrichtungen aus Dateien öffentlicher Stellen 54

5.2 Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherung bei den ADV-Einrichtungen der hessischen Hochschulen (Entwurf) 54

5.3 Richtlinien für die Tätigkeit der Schulpsychologen in der Abteilung Schulpsychologischer Dienst im Staatlichen Schulamt (Entwurf) 57

5.4 Rechtsvorschriften und veröffentlichte Erlasse zum Datenschutz und zur Datensicherung für den öffentlichen Bereich in Hessen 59

1. Zur Situation

1.1
Der Datenschutz befindet sich in einer zunehmend kritischen Phase. Gewiß, Schwierigkeiten hat es von Anfang an gegeben. Doch während bis vor kurzem jedenfalls über die Notwendigkeit einer gesetzlichen Regelung der Verarbeitung personenbezogener Daten Konsens bestand, mehren sich jetzt Zweifel und Kritik. Für manchen ist es sogar längst an der Zeit, sich offen von einer Gesetzgebung zu distanzieren, die, so heißt es, auf schwammigen Vorstellungen über die Interessen des Bürgers beruht, statt sich an der Realität der Verwaltung und an ihren Aufgaben zu orientieren. Die Beweiskette ist allem Anschein nach lang. Sie reicht von den ständig wiederkehrenden Hinweisen auf die schier endlose Auseinandersetzung über die "Jubiläumsdaten" bis hin zu der Behauptung, die ständigen Ermahnungen und Forderungen der Datenschutzbeauftragten würden letztlich nur die Verwaltungskosten steigern und die Verwaltungstätigkeit behindern.

Eines ist sicher richtig. Der Datenschutz zwingt jeden, der personenbezogene Daten verarbeiten möchte, dazu, seine bisherigen Arbeitsmethoden ebenso zu überprüfen wie seine Informationserwartungen. Genaugenommen verhält sich der Gesetzgeber nicht anders als es etwa das Bundesverfassungsgericht bei seiner Entscheidung über die Heranziehung von Scheidungsakten bei der Beurteilung eines Beamten getan hat (E 27,344). Hier wie dort werden dem Zugriff auf personenbezogene Daten Grenzen gesetzt. Hier wie dort steht die Überlegung im Vordergrund, daß eben nicht ohne weiteres auf alle erreichbaren Informationen zurückgegriffen werden darf, die Verwaltungstätigkeit sich also auch und gerade in Kenntnis der Informationsschranken abspielen muß.

Je deutlicher diese Grenzen formuliert werden, desto mehr macht sich Widerstand bemerkbar. Nur wäre es falsch, so zu tun, als ob die Kritik am Datenschutz nicht mehr widerspiegele als den Versuch, an überholten, keinesfalls mehr hinzunehmenden Vorstellungen festzuhalten. Was schon in früheren Tätigkeitsberichten gesagt worden ist, gilt nach wie vor: Der Datenschutz ist ein fortwährender Lernprozeß, und zwar keineswegs nur derjenigen, die sich bei ihrer Tätigkeit mit neuen Verhaltensregeln konfrontiert sehen. An diesem Lernprozeß sind auch und gerade diejenigen beteiligt, die für eine Verwirklichung der Datenschutzbestimmungen sorgen müssen. Kein Datenschutzbeauftragter kann ernsthaft von sich behaupten, sofort und für lange Zeit die Konsequenzen der gesetzlichen Regelung für die Vielzahl der konkreten Situationen eindeutig ziehen zu können, mit denen er sich auseinandersetzen muß. Genauso wie der Gesetzgeber seine Entscheidung als erste Annäherung an die Probleme der Verarbeitung personenbezogener Information verstanden hat, versucht auch der Datenschutzbeauftragte, die Konturen der jeweiligen Fragen immer schärfer herauszuarbeiten und damit auch immer präzisere Antworten zu geben. Er kann dieses Ziel aber nur erreichen, wenn er seine Aufgabe als konstanten Dialog mit dem Bürger und mit der Verwaltung begreift. Aus eben diesem Gespräch bezieht er seine Anregungen, und genau dieses Gespräch zeigt ihm auch, wo er nicht zuletzt die eigenen Entscheidungen korrigieren und verbessern muß. Wer deshalb im Datenschutzbeauftragten eine Instanz sieht, die belehrt und verkündet, geht von falschen Voraussetzungen aus. Die Grundbedingung der Tätigkeit des Datenschutzbeauftragten ist die Kooperation mit dem Bürger und der Verwaltung, die Fähigkeit zum Meinungsaustausch und die Bereitschaft, daraus zu lernen.

Schon deshalb geht es nicht an, den Datenschutz als Hindernis jeder vernünftigen Verwaltungstätigkeit darzustellen. Zudem: Solche Behauptungen halten, wie nicht zuletzt eine in Bremen durchgeführte Untersuchung gezeigt hat, einer genauen Überprüfung nicht stand. Das gilt bereits für die kostenmäßigen Auswirkungen des Datenschutzes. Er hat sicherlich in manchen Verwaltungsbereichen eine freilich geringe und letztlich nur zeitweilige Erhöhung der Ausgaben zur Folge gehabt. Schaut man aber genau hin, dann erweist sich sehr bald, daß die Mehrkosten zum größten Teil auf Maßnahmen der Datensicherung zurückzuführen sind. Anders ausgedrückt: Es geht um Ausgaben, die längst fällig gewesen wären, weil eine ordnungsmäßige Verwaltung auch ohne präzise Datenschutzanforderungen für eine sichere Aufbewahrung personenbezogener Daten zu sorgen hat. Soweit im übrigen Folgen für den Personalbereich entstanden sind, etwa durch die Wahrnehmung von Datenschutzaufgaben, gibt es genug organisatorische Möglichkeiten, die es ermöglichen, Kosten fast durchweg zu vermeiden. Aber auch sonst kann von einer Behinderung der Verwaltungstätigkeit nicht die Rede sein. Zwar ist nicht zu leugnen, daß die mit der gesetzlichen Regelung verbundenen Übermittlungssperren zumindest in der Anfangsphase dort Komplikationen verursacht haben, wo auf bestimmte, bislang verwendete Daten verzichtet oder ein umständlicherer Weg für den Informationszugang befolgt werden mußte. Mittlerweile hat sich aber gezeigt, wie sehr die Verwaltungsaufgaben auch mit dem geringeren Maß an Informationen erfüllt werden können und wie wenig letztlich die organisatorische Umstellung ins Gewicht fällt.

Ganz abgesehen davon muß sich jeder, der die Wirksamkeit der Verwaltung als Argument gegen den Datenschutz ins Feld führt, die Frage stellen, woran er denn eigentlich die Effizienz der Verwaltung wirklich mißt. Wie sich Verwaltung vollzieht, entscheidet sich in erster Linie an den in der Verfassung und den Gesetzen verankerten Grundsätzen über die Staatsstruktur und die Stellung des Bürgers. Wo sich aber die Verfassung, wie in der Bundesrepublik, für eine demokratische Struktur entscheidet, folgt daraus auch die radikale Absage an alle Tendenzen, den Bürger so perfekt wie möglich zu steuern, mögen sie im übrigen noch so wohlgemeint sein. Die Verwaltung hat sich, mit anderen Worten, nicht an die Stelle des Bürgers zu setzen, um für ihn zu entscheiden,

sondern sie muß ihre Tätigkeit dazu nutzen, um ihm die Chance zu geben, selbst darüber befinden zu können, wie seine Interessen zu verwirklichen sind. Mit dem Datenschutz reagiert der Gesetzgeber auf eine immer umfangreichere Verarbeitung personenbezogener Daten, die dank neuer und besserer Verarbeitungsverfahren die Steuerungsgefahren verschärft. So wenig sich die Notwendigkeit übersehen läßt, die Verwaltung gerade um der vielfältigen, im Interesse des Bürgers übernommenen Aufgaben willen zu informieren, so sehr kommt es darauf an, rechtzeitig für eine zweckgebundene, transparente und kontrollierbare Verarbeitung der Information zu sorgen. Nichts anderes will der Datenschutz, und eben deshalb sind seine Regeln Grundbedingung einer auf dem Respekt vor dem Bürger gegründeten Verwaltung. Die Wirksamkeit ihrer Tätigkeit muß sich unter diesen Umständen auch und gerade daran messen, wie dieser Bedingung Rechnung getragen wird.

Gerade daher gilt es freilich, mit dem Datenschutz vorsichtig umzugehen, seine Trivialisierung ebenso wie seine Bürokratisierung zu vermeiden. Wer sein Augenmerk nur auf die Jubiläumsdaten richtet, verliert alsbald den Blick für die Abhängigkeit und die Gefahren, die eine Verarbeitung einer immer vollständigeren Information über den einzelnen mit sich bringt. Und wer der Meinung ist, die Datenschutzkontrolle ohne jenen schon erwähnten Dialog mit dem Bürger und mit der Verwaltung verwirklichen zu können, handelt dem Datenschutzbeauftragten zu Recht den Vorwurf ein, nichts anderes bewirkt zu haben, als die Probleme zu verwalten, statt sich mit ihnen wirklich auseinanderzusetzen und nach überzeugenden Lösungen zu suchen.

1.2

Kritisch ist die Situation des Datenschutzes aber auch deshalb, weil der Zeitpunkt gekommen ist, zu dem sich erweisen muß, ob es gelingen kann, die in den letzten Jahren gewonnenen Erfahrungen in neue und bessere gesetzliche Vorschriften umzusetzen. Die Novellierung des BDSG steht unmittelbar bevor, ein Vorgang, der keineswegs nur den Bundesgesetzgeber etwas angeht. Die Entwicklung des Datenschutzes in der Bundesrepublik ist durch die Wechselwirkung von Landes- und Bundesgesetzgebung gekennzeichnet. Am Anfang stand das Hessische Datenschutzgesetz von 1970; am vorläufigen Ende findet sich ein Normenkomplex, der sich keineswegs in den Vorschriften des BDSG erschöpft, sondern die Bemühungen der Länder widerspiegelt, in ihrem Kompetenzbereich weiterzugehen und für einen wirksameren Datenschutz zu sorgen. Die schärfere Zweckbindung, die Gebührenfreiheit, die präziseren Übermittlungssperren, der Schadensersatz sind Beispiele dafür. Eben diesen Prozeß der gegenseitigen Beeinflussung greift die Novellierung auf und setzt ihn fort. Das korrigierte BDSG wird zwangsläufig auch der Ausgangspunkt für Korrekturen der Landesdatenschutzgesetze sein. Um so mehr kommt es darauf an, rechtzeitig die für eine Reform entscheidenden Vorstellungen zu formulieren.

Freilich gilt es, sich auch von Anfang an der Grenzen einer Novellierung bewußt zu sein. Die Novellierung ist Korrektur des 1976 verabschiedeten Bundesdatenschutzgesetzes. Sie erfolgt insofern vor dem Hintergrund einer bestehenden gesetzlichen Regelung und vollzieht sich in einem durch diese Regelung weitgehend vorgegebenen Rahmen. Man kann sicherlich nach wie vor darüber streiten, ob es nicht ein anderes und besseres Regelungssystem gibt als das des BDSG. Nicht zuletzt die jüngsten Diskussionen im Europäischen Parlament haben deutlich gezeigt, daß der vom BDSG beschrittene Weg keineswegs der einzig mögliche oder gar der einzig richtige ist. Vielmehr gibt es durchaus gewichtige Argumente zugunsten einer Regelung, die genau den umgekehrten Weg geht, bereichsspezifisch also ansetzt und deshalb auch gezielt die Vorteile einer Lizensierung der Datenverarbeitung nutzt. Nur steht nicht die Revision der Grundentscheidung des Gesetzgebers zur Debatte, sondern lediglich die Verwirklichung dieser Entscheidung. Die einzelnen Antworten, die er versucht hat, auf die Datenschutzfragen zu geben, sind mithin Ansatzpunkt der Novellierung und bestimmen ihre Richtung.

Gerade deshalb ist allerdings die Versuchung groß, die Novellierung als Generalüberholung zu verstehen, also den Gesetzestext Vorschrift für Vorschrift durchzugehen, um sämtliche in der Zwischenzeit sichtbar gewordenen Probleme aufzugreifen. Eine so gesehene Novellierung riskiert freilich, sich in einer Vielzahl von Details zu verlieren und letztlich als sinnloser Streit von Spezialisten abgetan zu werden. Reform kann unter diesen Umständen nur sorgsame Gewichtung der Erfahrungen und Vorschläge bedeuten mit der Konsequenz einer gezielten Konzentration auf Schwerpunkte. Die Überzeugungskraft der Novellierung hängt auch und gerade von der Zurückhaltung des Gesetzgebers ab. Mehr Korrekturmöglichkeiten anzugeben, ist keine Kunst, sich auf die zentralen Punkte zu einigen und zu beschränken, weitaus schwieriger. Noch einmal freilich: Nur unter dieser Voraussetzung kann es gelingen, sich nicht auf Nebenfelder abdrängen zu lassen und nur noch über Formulierungen zu streiten, dort, wo es in Wirklichkeit um die Substanz des Datenschutzes geht. Die Konzentration auf bestimmte Schwerpunkte ist auch deshalb notwendig, weil sonst einer der wichtigsten Aspekte der Entwicklung des Datenschutzes seit der Verabschiedung des BDSG gefährdet werden könnte: die fortschreitende Ergänzung und Präzisierung der BDSG-Normen durch bereichsspezifische Vorschriften.

Die Kritik an den viel zu allgemein gehaltenen Bestimmungen des BDSG ist nicht ohne Wirkung geblieben. Der Gesetzgeber hat in einer ganzen Reihe von Fällen die vagen Formulierungen des BDSG verdrängt und an ihrer Stelle Regeln vorgesehen, die sich an konkreten Verarbeitungssituationen orientieren und deshalb weitaus präzisere Antworten auf die Datenschutzfragen zu geben suchen. Die Datenschutzbestimmungen des Melderechts sind ebenso ein Beispiel dafür wie die Sonderregelungen des Sozialgesetzbuches. Man kann gewiß auch bei diesen

Vorschriften über manches Detail streiten. Man kann aber nicht in Abrede stellen, daß mit ihrer Hilfe der Datenschutz eine sehr viel verbindlichere Gestalt gewinnt, seine Konsequenzen deutlicher zu erkennen sind und seine Wirksamkeit daher zunimmt. Gerade deshalb gilt es, jeden Rückfall in die Vorstellung zu vermeiden, man könne in einem Gesetz eine überzeugende Lösung aller Datenschutzprobleme bringen. Das BDSG formuliert eine erste Grundlage für eine Verarbeitungsregelung und nicht die abschließende Antwort des Gesetzgebers auf die Datenschutzprobleme. Die Novellierung ist deshalb weder ein Ersatz für die bereichsspezifische Regelung des Datenschutzes, noch darf sie zum Hindernis für weitere Anstrengungen einer bereichsspezifischen Präzisierung werden.

Schwerpunkte setzen heißt freilich nicht, bestimmte Regelungsbereiche des BDSG von vornherein außer Betracht zu lassen. Die Novellierung muß im Gegenteil ebenso wie das BDSG den Datenschutz als eine Aufgabe sehen, die sich bei jeder Verarbeitung personenbezogener Daten stellt, den öffentlichen also genauso wie den privaten Bereich betrifft. Wenn hier darauf besonders verwiesen wird, so deshalb, weil Bundes- und Landesgesetzgeber durch ihre Regelungen eine Entwicklung gefördert haben, die den Eindruck erweckt, als ob der Datenschutz, wenn nicht ausschließlich, so doch weitgehend ein Problem der öffentlichen Verwaltung ist. Die Einrichtung besonderer, unabhängiger Kontrollinstanzen für den öffentlichen Bereich, die alljährlichen Berichte der Datenschutzbeauftragten an die Parlamente und die damit verbundene öffentliche Diskussion lenken mehr oder weniger zwangsläufig die Aufmerksamkeit auf die öffentliche Verwaltung. Nur zu verständlich ist es aber dann, wenn die im privaten Bereich sichtbar gewordenen Konflikte in den Hintergrund geraten, ganz gleich ob es sich um den Schutz der Arbeitnehmerdaten, die Übermittlung von Informationen im Kreditbereich oder die Verarbeitung der Daten von Versicherungsnehmern handelt. Die Novellierung darf an diesen Problemen, jedenfalls soweit sie das BDSG berühren, genausowenig vorbeigehen wie an den verschiedenen für den öffentlichen Bereich wichtigen Fragestellungen. Kurzum, eine Novellierung, die den Datenschutz nicht verzerrt, sondern nach wie vor die Verarbeitungsgefahren in den Mittelpunkt stellt, kann keinen Bereich des BDSG von der Korrektur ausnehmen.

1.3
Bleibt ein letzter Gesichtspunkt, der nicht minder Beachtung verdient, wenn die Lage des Datenschutzes richtig eingeschätzt werden soll. Der Gesetzgeber hat sich unstreitig bemüht, den Datenschutz durch gezielt bereichsspezifische Vorschriften wirksamer zu gestalten. Das Sozialgesetzbuch bietet mit seinen auch in diesem Tätigkeitsbericht wieder behandelten Bestimmungen (unten 4.1) zum Sozialgeheimnis ein gutes Beispiel dafür. Um so mehr muß die Art und Weise erstaunen, ja befremden, in der in letzter Zeit diese als unentbehrlich bezeichneten Informationsbarrieren vom Gesetzgeber selbst durchbrochen worden sind (dazu unter 4.1.4). Wohlgemerkt, es kann durchaus Situationen geben, in denen es gerechtfertigt erscheint, den Zugriff auf die Sozialdaten über den Kreis der ursprünglich vorgesehenen Fälle hinaus zu erlauben. Soweit aber wirklich überzeugende Gründe dafür vorliegen, muß der Gesetzgeber von vornherein darauf bedacht sein, den Zweck der Durchbrechung unmißverständlich zu umschreiben, jede Formulierung also zu vermeiden, die eine Ausweitung des Zugriffs begünstigen könnte. Eben dies ist nicht geschehen. Die Glaubwürdigkeit des Sozialgeheimnisses, aber auch des Datenschutzes überhaupt ist damit gefährdet. Wie verläßlich Informationsbarrieren sind, hängt auch und gerade von der Bereitschaft des Gesetzgebers ab, die Schranken zu respektieren, die er selbst geschaffen hat.

1.4.
Seit der Verabschiedung des ersten Hessischen Datenschutzgesetzes ist mittlerweile mehr als ein Jahrzehnt vergangen. Anlaß genug, um einige kurze Bemerkungen zur Organisation des Amtes zu machen. Sie ist durch Vorstellungen geprägt, die bereits in den allerersten Jahren entstanden sind. Der Datenschutzbeauftragte trägt ohne Zweifel die Verantwortung für die vom Gesetz geforderte Kontrolle. Die Entscheidung über den jeweils einzuschlagenden Weg liegt ausschließlich bei ihm; er hat deshalb auch für alle Vorschläge und Beanstandungen einzustehen. Nur wäre es falsch, ihn allein zu sehen und deshalb auch zu meinen, was auch immer im Datenschutzbereich geschehe, sei die Folge seiner Anregungen und der darauf gegründeten Anordnungen. Der Datenschutzbeauftragte steht vielmehr an der Spitze eines Amtes, das seine Aufgabe nur erfüllen kann, solange von allen Mitarbeitern die Fähigkeit zur Eigeninitiative ebenso verlangt wird wie die Bereitschaft zur Kooperation. Anders ausgedrückt: Ganz gleich, ob es um einzelne Überlegungen zum Datenschutz oder den jährlich abzugebenden Bericht geht, beides entsteht aus einem Diskussionsprozeß, in den alle Referenten ihre Erfahrungen einbringen und gemeinsam Vorstellungen formulieren.

Gerade deshalb ist schon sehr früh darauf hingewiesen worden, daß wirksamer und überzeugender Datenschutz keineswegs mit einer ständig zunehmenden Zahl von Mitarbeitern zusammenhängt, sondern im Gegenteil eine klare Begrenzung voraussetzt, die in den Haushaltsberatungen mit der Zahl von acht Mitarbeitern präzisiert wurde. Nur unter dieser Bedingung kann es in der Tat gelingen, ein Organisationsmodell zu verwirklichen, das auf gleichberechtigter kollegialer Zusammenarbeit beruht und damit zugleich eine durch hierarchische Strukturen bedingte Bürokratisierung des Datenschutzes vermeidet.

In diesem Zusammenhang ist auch darauf hinzuweisen, daß die Aufgaben des Hessischen Datenschutzbeauftragten spätestens seit der Verabschiedung des zweiten Hessischen Datenschutzgesetzes 1978 erheblich zugenommen haben. Neben der automatischen muß auch die manuelle Datenverarbeitung kontrolliert werden; entsprechend intensiver und umfangreicher fallen die Prüfungsaufgaben aus. Was das bedeutet, zeigt etwa die Zahl von gegenwärtig ca. 6.000 im Register aufgenommenen Dateien. Darüberhinaus nimmt der Datenschutzbeauftragte weitaus mehr als bisher Aufgaben der Fortbildung der Mitarbeiter des öffentlichen Dienstes wahr. Allein im letzten Jahr nahmen meine Mitarbeiter und ich an über hundert Informations- und Weiterbildungsveranstaltungen zum Datenschutz teil.

Um so bedauerlicher ist es, daß die Zahl der acht Mitarbeiter immer noch nicht erreicht werden konnte. Sicher muß auch der Datenschutzbeauftragte Einsparungen in Kauf nehmen. Dazu sind auch konkrete Vorschläge gemacht worden. Nur rechtfertigen es die notwendigen Einsparungen nicht, auf die fehlenden zwei Referenten zu verzichten, und zwar vor allem auf die wiederholt geforderte Einstellung eines Informatikers. Das Gesetz schreibt dem Datenschutzbeauftragten vor, auch und gerade die Entwicklung der Verarbeitungstechnik zu verfolgen und verlangt ebenso von ihm, den Gesetzgeber auf die notwendige Fortschreibung der Datensicherung aufmerksam zu machen. Dies setzt ebenso spezialisierte wie kontinuierlich aktualisierte Kenntnisse der technischen Entwicklung voraus, um die Arbeit des Datenschutzbeauftragten auf dem neuesten Stand der DV-Technik zu halten. Eine weitere Verzögerung muß sich insofern nachteilig auf die Kontrolle auswirken und die korrekte Erfüllung der gesetzlichen Aufgaben gefährden.

1.5
Anders als bisher enthält der diesjährige Tätigkeitsbericht eine Bilanz (vgl. unten 2.). Damit wird zum ersten Mal versucht, klarzustellen, welche Wirkungen die früher gemachten Vorschläge gehabt haben, wo also eine Verbesserung des Datenschutzes erzielt werden konnte und wo es an einer Regelung nach wie vor fehlt. Auf die Bilanz folgt ein besonderer Abschnitt, der ähnlich wie im letzten Bericht verdeutlichen soll, welches die wichtigsten Aufgaben für das kommende Jahr sind(vgl.unten 3.). Den Abschluß bilden Überlegungen zu bestimmten, für die Entwicklung des Datenschutzes besonders wichtigen Problembereichen. Sie beruhen auf den im Berichtszeitraum gewonnenen Erfahrungen(vgl. unten 4.).

2. Bilanz

2.1
Zum 7. Tätigkeitsbericht für 1978 (Drucks. 9/67)

2.1.1
Vorsorgeuntersuchung Vorsorgeuntersuchung bei der Einschulung

Der 7. Bericht enthielt u.a. Bedenken gegen das Verfahren der "Schulreifeuntersuchung" (8.2.). Die Stellungnahme der Landesregierung (Drucks. 9/904, 2.6.2) ging nur auf einige Kritikpunkte ein. Beschwerden von Eltern, die auch in den Jahren 1979 und 1980 wiederholt eingingen, lieferten den Beweis dafür, daß nach wie vor Mängel bei der Handhabung der Einschulungsuntersuchung auftraten. Nach einer Reihe von Interventionen beim Hessischen Sozialminister erging nach eingehender Beratung mit mir am 19. Januar 1981 ein Erlaß (Az. III A 2/3 - 18 h 12/05) an alle Gesundheitsämter und deren Aufsichtsbehörden. Dieser Erlaß führt landeseinheitlich ein Untersuchungsverfahren nach neuen Arbeitsrichtlinien ein und enthält Regelungen, die - wenn sie eingehalten werden - eine aus der Sicht des Datenschutzes ordnungsgemäße Verfahrensweise gewährleisten.

So legt der Erlaß u.a. fest:

- Die Eltern werden darauf hingewiesen, daß das Ausfüllen des an sie versandten Anamnesefragebogens für die Kinder ("Elternfragebogen") freiwillig ist - im Gegensatz zur Schulreifeuntersuchung selbst, die nach § 42 Abs. 2 SchulverwaltungsG obligatorisch ist. § 11 Abs. 2 HDSG verlangt einen Hinweis auf die Freiwilligkeit immer dann, wenn Daten beim Betroffenen erhoben werden, ohne daß dies eine Rechtsvorschrift erlaubt.
- Nach Abschluß der Schulgesundheitspflege sind die Schulgesundheitsbögen mit einem Sperrvermerk zu versehen. Dies verlangt § 19 Abs. 2 HDSG, nach dem für die Aufgabenerfüllung nicht mehr benötigte Daten zu sperren sind. Dem Gebot der Zweckbindung folgend darf das Gesundheitsamt während der zehnjährigen Aufbewahrungszeit die Befunde aus den Bögen nur zu Zwecken der Schul- und Jugendgesundheitspflege heranziehen, es sei denn, es liegt die Zustimmung des Betroffenen oder seiner Erziehungsberechtigten zu anderweitiger Verwendung vor. Nach Ablauf dieser Aufbewahrungsfrist sind die Bögen zu vernichten, wenn der Betroffene nicht mit dem weiteren Gebrauch einverstanden ist.
- Für Kindergartenuntersuchungen gelten die genannten Grundsätze entsprechend.

Erlasse sind nur so gut, wie sie in der Verwaltungspraxis der Behörden angewandt und umgesetzt werden. Für den Datenschutzbeauftragten ist es nie damit getan, durch Vorschläge und Anregungen Ministerien zu einem aus der Sicht des Datenschutzes begrüßenswerten Erlaß zu veranlassen. Beratung und Kontrolle ergänzen sich. Bei stichprobenweiser Kontrolle der Formulargestaltung einzelner Gesundheitsämter in Hessen konnte ich mich davon überzeugen, daß die Vordrucke - soweit ersichtlich - dem neuen Erlaß entsprechend ausgestaltet sind.

2.2.
Zum 8. Tätigkeitsbericht für 1979 (Drucks. 9/2740)

2.2.1
Wissenschaftliche Forschung und Datenschutz

§ 15 HDSG ist nur ein erster Schritt auf dem Weg zur Lösung möglicher Konflikte zwischen Datenschutz und Datenzugang für Forschungszwecke (1.2.4, 2.1.7).

Der Hessische Landtag hatte in diesem Zusammenhang den Hessischen Kultusminister und den Hessischen Innenminister gebeten, Richtlinien zur Konkretisierung des § 15 HDSG zu formulieren (Drucks. 9/2740, PL 47/9 vom 11.12.1980). Der Erlaß vom 13.6.1981 (StAnz. S. 1262, vgl. den Text unten 5.1) ist das Ergebnis intensiver Gespräche zwischen den beteiligten Ressorts und meiner Dienststelle. Er legt Voraussetzungen für eine Übermittlung personenbezogener Daten durch Behörden an Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe wissenschaftlicher Forschung fest. Erleichtert wurde vor allem die - für Projekte der empirischen Sozialforschung wichtige - Ziehung von Repräsentativstichproben. Zugleich stellt der Erlaß im Interesse des Bürgers, dessen Name und Anschrift weitergegeben werden, Bedingungen für die Erhebung von Daten beim Betroffenen und für die Verarbeitung zu Forschungszwecken auf. Er macht deutlich, daß eine Übermittlung dann nicht die schutzwürdigen Belange der Betroffenen beeinträchtigt, wenn die Forschungseinrichtung die Daten unverzüglich nach Erhalt anonymisiert.

2.2.2
Kriminalpolizeiliche Sammlungen

Mit zu den wichtigsten Ansätzen für eine rechtliche Regelung der Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden gehören die "Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen" (KpS-Richtlinien). Ich hatte seinerzeit moniert (1.2.1), daß diese Richtlinien für Hessen noch nicht erlassen waren, obwohl sie zum Teil von anderen Bundesländern sowie vom Bundesminister des Innern für das Bundeskriminalamt bereits in Kraft gesetzt worden waren.

Der Hessische Landtag beschloß daraufhin in seiner Sitzung vom 11.12.1980 - einer Empfehlung des Innenausschusses folgend - "... die Landesregierung zu bitten, auf eine baldige Beschlußfassung hinsichtlich der KpS-Richtlinien (bei der Innenministerkonferenz) zu drängen und die KpS-Richtlinien dann in Kraft zu setzen, wenn die Beschlußfassung nicht bis zum Frühjahr nächsten Jahres (d.h. 1981) erfolgt" sei.

Der Hessische Innenminister ist dieser Bitte mit dem Erlaß vom 19.3.1981 (StAnz. S. 881) nicht nur gefolgt, sondern hat auch Änderungen am Entwurf vorgenommen, die meinen Forderungen zur Verbesserung des Datenschutzes entgegenkommen. So sind beispielsweise die Prüffristen zur Aussonderung bzw. Löschung bei Daten von Kindern und Jugendlichen erheblich verkürzt worden. Sie betragen in den hessischen Richtlinien bei Kindern 1 Jahr (dagegen KpS-Richtlinien Bund: 2 Jahre), bei Jugendlichen 2 Jahre (Bund: 5 Jahre) und bei anderen Personen 3 Jahre (Bund: 10 Jahre), sofern die Fälle von geringer Bedeutung sind und nicht inzwischen neue Eintragungen erfolgt sind (vgl. Ziff. 5.2.2).

2.3
Zum 9. Tätigkeitsbericht für 1980 (Drucks. 9/4032)

2.3.1
Direktverbindung zwischen Polizei und Kfz-Zulassungsstelle

Der 9. Tätigkeitsbericht stellte ausdrücklich fest, daß der Direktzugriff der Polizei über einen eigenen Bildschirm auf die Dateien der Kfz-Zulassungsstellen mit § 26 Abs. 5 StVZO nicht zu vereinbaren ist (2.1.1). Eine Datenübermittlung darf nach dieser Vorschrift nur "auf Antrag im Einzelfall" erfolgen. Die Landesregierung ist dieser Ansicht in ihrer Stellungnahme zum Tätigkeitsbericht (Drucks. 9/4479) entgegengetreten (zu 2.1.1). Nachdem die Einführung des Direktzugriffs in diesem Jahre auf eine Reihe weiterer Landkreise ausgedehnt wurde, beanstandete ich dieses Verfahren förmlich gem. § 26 Abs. 1 HDSG. Der Hessische Minister des Innern wies diese Beanstandung zurück.

Nach seinem Beschluß vom 23.6.1981 (Drucks. 9/4880) hält es der Hessische Landtag für wünschenswert, die Zulässigkeit von Direktzugriffsverfahren auf eine einwandfreie rechtliche Grundlage zu stellen, in der der Anlaß, der Zweck der Übermittlungen, die Datenempfänger und die zu übermittelnden Daten jeweils festzulegen sind. Der Landtag hält zwar die derzeitige Praxis für vertretbar, fordert aber die Landesregierung auf, unter Beachtung der Maßnahmen in anderen Bundesländern und der Diskussion auf Bundesebene eine entsprechende Präzisierung der Bestimmungen der StVZO herbeizuführen

Da es sich beim Direktzugriff um ein generelles datenschutzrechtliches Problem handelt, habe ich nicht zuletzt im Hinblick auf die Novellierung des BDSG eine Neufassung der §§ 10 und 11 BDSG vorgeschlagen, die unter bestimmten Voraussetzungen die Einrichtung von Direktzugriffsverfahren zuläßt (vgl. unten 3.2.4.2.2).

2.3.2
Neuregelung des Datenschutzes im Hessischen Krankenhausgesetz

Zur Verbesserung des Schutzes von Patientendaten im Krankenhaus hatte ich eine entsprechende Novellierung des Hessischen Krankenhausgesetzes vorgeschlagen (2.2.1). Die Landesregierung hat sich in ihrer Stellungnahme (Drucks. 9/4479, zu 2.2.1) nicht nur damit einverstanden erklärt, sondern auch mitgeteilt, sie werde die Möglichkeit untersuchen, über den Krankenhausbereich hinaus weitere Gebiete des Gesundheitswesens in eine umfassende Datenschutzregelung einzubeziehen.

Zu diesem Komplex hat bisher lediglich ein erster Meinungsaustausch mit dem Hessischen Sozialminister stattgefunden (September 1981). Mir ist nicht bekannt, ob der Hessische Sozialminister seine Vorbereitungsarbeiten in diesem Bereich fortgeführt hat und wann mit der Vorlage eines Gesetzentwurfs gerechnet werden kann.

Besonderes Gewicht erhält der Schutz von Patientendaten in der nächsten Zukunft deshalb, weil - aufgrund von Beschlüssen des Kommunalen sowie des Landes-Automationsausschusses - die Entwicklung einer Konzeption für die DV-Unterstützung des Betriebs hessischer Krankenhäuser zügig vorangetrieben werden soll.

2.3.3
Krebsregister

Der Hessische Landtag hat am 23.6.1981 zu dem Berichtsabschnitt über das Krebsregister (2.2.2) folgenden Beschluß gefaßt: "Der Landtag ist der Auffassung, daß die Durchführung der Pilotstudie zur Einführung eines Krebsregisters nur dann zulässig ist, wenn die vorgesehenen Datensicherungsmaßnahmen unverzüglich getroffen werden und eine gesetzliche Grundlage bis zum Jahresende vorliegt." (Drucks. 9/4880; Plenarprotokoll 9/58).

Im Oktober hat zwischen dem Hessischen Sozialminister und mir ein erstes Gespräch auf Referentenebene über den Vorentwurf eines Krebsregistergesetzes stattgefunden. Dieser Vorschlag beruhte auf dem Modellentwurf eines Krebsregistergesetzes, den eine Arbeitsgruppe der von der Bundesregierung einberufenen "Großen Krebskonferenz", an der auch ich beteiligt war, formuliert hat.

Beim Hessischen Sozialminister ist es aber offensichtlich bisher bei hausinternen Überlegungen geblieben. Die Landesregierung hat jedenfalls bis Ende Dezember 1981 dem Landtag keinen Gesetzentwurf zugeleitet. Von ihr sind darüberhinaus keine Vorstellungen entwickelt worden, wie der Aufbau des Krebsregisters ohne gesetzliche Grundlage fortgesetzt werden soll.

Hinzu kommt, daß die von mir beanstandeten Mängel der Gebäudesicherung im Rechenzentrum der Universität Gießen, in dem die Daten des Krebsregisters verarbeitet werden, noch immer nicht behoben sind. Eine Stellungnahme des Hessischen Kultusministers zu meiner Beanstandung vom 20.5.1981 liegt mir bis heute ebenfalls nicht vor.

2.3.4
Datenverarbeitung durch den Verfassungsschutz

Der ausführliche Vorschlag für ein neues Hessisches Verfassungsschutzgesetz (2.4) ist bisher folgenlos geblieben. Dies ist umso bedauerlicher, als die Landesregierung in ihrer Stellungnahme zu meinem Bericht erklärt hat, "daß Aufgaben und Befugnisse des Landesamtes für Verfassungsschutz unter Berücksichtigung datenschutzrechtlicher Belange neu geregelt werden sollten" (Drucks. 9/4479, zu 2.4). Die an gleicher Stelle enthaltenen Überlegungen, wegen des engen Zusammenhanges von Bundes- und Landesgesetzgebung in diesem Bereich ein neues Hessisches Verfassungsschutzgesetz solange nicht zu verabschieden, bis der Bundesgesetzgeber auf diesem Gebiet aktiv wird, überzeugt nicht: Andere Länder haben bereits neue Gesetze, so seit 1981 Bremen und Nordrhein-Westfalen. In diesem Zusammenhang muß noch einmal darauf hingewiesen werden, daß die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Bereich des Landesamtes für Verfassungsschutz zumindest zweifelhaft ist. Klare gesetzliche Befugnisnormen sind deshalb unerläßlich.

2.3.5.
Das Melderechtsrahmengesetz und die Novellierung des Landesmelderechts

Im Melderechtsrahmengesetz des Bundes vom 23. August 1980 (BGBl. I S. 1429) wurde der Landesgesetzgeber aufgefordert, bis zum 23. August 1982 eine entsprechende gesetzliche Regelung zu verabschieden. Der hessische Entwurf für ein Landesmeldegesetz wurde mittlerweile im Kabinett beraten. Die im Tätigkeitsbericht (3.1) enthaltenen Vorschläge sind in die Vorarbeiten zu diesem Gesetz einbezogen worden. Insbesondere im Hinblick auf den im Melderegister zu speichernden Datensatz und die Verwendung von Ordnungsmerkmalen bringt der jetzt vorgelegte Entwurf zufriedenstellende Lösungen.

2.3.6
Datenschutz im Hochschulbereich

Die Prüfung der Universität Frankfurt hatte die Notwendigkeit unterstrichen, eine generelle Datenschutzregelung für die hessischen Hochschulen auszuarbeiten (4.3.6).

Inzwischen hat eine Arbeitsgruppe aus Vertretern der Hochschulen, des Hessischen Kultusministers sowie meiner Dienststelle einen Entwurf für "Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherung bei den ADV-Einrichtungen der hessischen Hochschulen" vorgelegt (vgl. den Text unten 5.2). Damit soll die "Dienstanweisung zur Gewährleistung des Datenschutzes und der Datensicherung im Hessischen Datenverarbeitungsverbund (DASCH)" den spezifischen Verarbeitungsbedingungen an den Hochschulen angepaßt werden. Einerseits wird der für die Kommunalen Gebietsrechenzentren festgelegte Sicherungsstandard entsprechend übernommen, andererseits eine Forschung und Lehre beeinträchtigende übermäßige Reglementierung vermieden.

Der Entwurf unterscheidet diejenigen ADV-Anlagen, auf denen personenbezogene Daten verarbeitet werden, von denen, die zur Verarbeitung naturwissenschaftlich-technischer oder Strukturdaten benutzt werden (einschließlich der Prozeßrechner). Nur die ersteren unterliegen den Richtlinien; Voraussetzung für ihren Betrieb ist eine besondere Zulassung. Diese behördeninterne "Lizensierung" von ADV-Einrichtungen ist als Regelungsmodell in der Bundesrepublik bisher einzigartig. Seine Verwirklichung hängt allerdings von einer genauen Inventarisierung der Geräteausstattung jeder Hochschule ab, da erst auf diese Weise der notwendige Überblick über Art und Umfang der Informationsverarbeitung und die vorhandenen technischen Einrichtungen gewonnen werden kann. Der Hessische Landtag hat gleichfalls eine vollständige Inventarliste des gesamten DV-Anlagenbestandes der hessischen Hochschulen bis zum Jahresende gefordert (Drucks. 9/4880; PL 58/9). Der Hessische Kultusminister ist bisher dieser Aufforderung nicht nachgekommen. Als Grund hierfür hat er die mangelnde Mitwirkung einzelner Hochschulen angeführt. Nicht zuletzt deshalb kann ich meine Kontrollaufgabe im Hochschulbereich insoweit nur unzureichend wahrnehmen.

2.3.7
Datensicherung - Forderungen an Automationsvorhaben der Verwaltung (vgl.4.6)

Im Sommer 1980 hatte ich den Landesautomationsausschuß (LAA) und den Kommunalen Automationsausschuß (KAA) aufgefordert, dafür zu sorgen, daß bei Automationsvorhaben der Landes- und Kommunalverwaltung die gemäß den DV-Leitsätzen vorzulegenden Berichte präzise Aussagen zu Maßnahmen des Datenschutzes und der Datensicherung enthalten. Der LAA hat daraufhin einen Beschluß gefaßt (96-10), nach dem Vertreter des Hessischen Ministers des Innern (Datenschutzreferat), des Hessischen Ministers für Wirtschaft und Technik, der Hessischen Zentrale für Datenverarbeitung und meiner Dienststelle eine Art "Checkliste" zum Datenschutz und zur Datensicherung erarbeiten sollten, die bei der Aufgabenuntersuchung als Hilfestellung herangezogen werden kann.

Diese Arbeitsgruppe hat inzwischen dem LAA einen solchen Katalog vorgelegt (Beschluß 106-4). Der Hessische DV-Verbund wird als Ergänzung zu dieser Liste eine "Benutzerordnung" veröffentlichen, die unter anderem die Standardlösungen zu Datenschutz- und Datensicherungsmaßnahmen aufzeigt, die die Rechenzentren des Hessischen DV-Verbundes den Verwaltungen anbieten, die neue DV-Verfahren einführen wollen.

3. Aufgaben

3.1.
Novellierung des Bundesdatenschutzgesetzes (BDSG)

3.1.1
Notwendigkeit der Reform

Die Reform des BDSG nimmt immer konkretere Gestalt an. Eigentlich stand die Notwendigkeit, das Gesetz zu novellieren, schon bei seiner Verabschiedung fest. Doch so sehr Konsens darüber bestand, daß der Gesetzgeber nicht mehr geleistet hatte als eine erste Annäherung an eine überzeugende Auseinandersetzung mit den Gefahren der Verarbeitung personenbezogener Daten, so schwer fiel es, die Novellierungsabsicht in konkrete Vorschläge umzusetzen. Was sich bei der Beratung des BDSG bereits andeutete, bewahrheitete sich in der Folgezeit immer mehr: Es gibt wenig Fälle, in denen der Gesetzgeber vor einer so komplizierten Aufgabe gestanden hat und nach wie vor steht.

Sicher, manches hat sich mittlerweile gebessert, weil nicht zuletzt dank der gesetzlich vorgeschriebenen Kontrolle der Verarbeitung eine ganze Reihe von Erfahrungen gewonnen werden konnte, die es ermöglicht, die Anforderungen an die Verarbeitung sehr viel präziser zu formulieren. Noch immer kommt es aber vor allem darauf an, mögliche Entwicklungen offenzulegen, ihre Konsequenzen für den Bürger zu erkennen und wirksame Gegenmittel zu finden. Der Wandel von der gleichsam normalen Übermittlung personenbezogener Daten zum automatisch gesteuerten Direktzugriff ist bezeichnend dafür. Ein Datenschutzgesetz, das die konstante technische Veränderung der Verarbeitung nicht einzufangen sucht, bleibt letztlich wirkungslose Spielerei. Je mehr es sich aber auf die möglichen Entwicklungen einläßt, desto schwieriger erweist es sich, ebenso präzise wie wirksame Regeln zu formulieren.

Trotzdem zeichnen sich für die Reform bestimmte Minimalforderungen ab, die allesamt darauf abzielen, die Aufgabe des Datenschutzes verständlicher zu machen, die Verarbeitungsbedingungen genauer zu gestalten und die Verarbeitungskontrolle wirksamer werden zu lassen.

3.1.2
Novellierungsbedürftige Vorschriften

3.1.2.1
Aufgabe des Datenschutzes

Gerade wenn die Novellierung als Mittel zur Korrektur und Fortschreibung des BDSG gesehen und verstanden wird, kommt es ganz besonders darauf an, das Gesetz von Mißverständnissen und Fehlinterpretationen zu entlasten, die seine Anwendung immer wieder in Frage stellen. § 1 Abs. 1 BDSG ist ein Musterbeispiel dafür. Die überaus schwerfällige und umständliche Formulierung provoziert förmlich Fehlschlüsse. Weder der Ausgangspunkt des Gesetzes - die mit der Verarbeitung personenbezogener Daten verbundenen Gefahren - noch sein Ziel -der Schutz des Einzelnen vor eben diesen Gefahren gelangen deutlich zum Ausdruck. Nicht von ungefähr haben deshalb manche Landesdatenschutzgesetze davon abgesehen, die Formulierung des § 1 BDSG zu übernehmen und statt dessen, wie etwa § 1 HDSG, ausdrücklich den Schutz des Bürgers in den Mittelpunkt gestellt. Ebensowenig geht es an, den Datenschutz als die Reaktion des Gesetzgebers auf irgendwelche Mißbräuche auszugeben. Das Gesetz ist nicht aus der Auseinandersetzung mit ganz bestimmten "Mißbräuchen" der Verarbeitung entstanden. Seine Vorschriften sind deshalb auch nicht als Vorwurf an die Adresse einzelner öffentlicher oder privater Instanzen zu verstehen. Dem Gesetzgeber ging und geht es vielmehr allein um die Gefahren, die eine Verarbeitung personenbezogener Daten für den einzelnen mit sich bringt, vom jederzeitigen und unbeschränkten Zugang bis hin zur unbeschränkten Kombinierbarkeit. Deshalb stellt das Gesetz Verarbeitungsbedingungen auf, deshalb gewährt es dem Betroffenen Informations- und Korrekturrechte, und deshalb spricht es sich schließlich für eine Kontrolle der Verarbeitung durch eigens dafür vorgesehene Instanzen aus. Von einer korrekten und vor jedem Mißverständnis gefeiten Aufgabendefinition des Datenschutzes kann daher nur so lange die Rede sein, wie sie feststellt, daß es Aufgabe des Datenschutzes ist, den einzelnen vor den Gefahren zu schützen, die mit einer Verarbeitung der sich auf seine Person beziehenden Daten verbunden sind.

3.1.2.2
Zweckbindung

Bundes- und Landesdatenschutzgesetze bringen deutlich zum Ausdruck, daß ein wirksamer Datenschutz mit einer Einschränkung der Verarbeitung untrennbar zusammenhängt. Der Gesetzgeber grenzt daher die Verwendung gezielt ein: nicht die jeweils gewünschten, sondern immer nur die erforderlichen Daten dürfen verarbeitet werden. Doch damit ist nur eine wichtige Schranke aufgerichtet. Eine weitere, genauso bedeutsame Barriere ist die strikte

Zweckbindung. Sie schließt die bei einer automatischen Verarbeitung besonders naheliegende Gefahr einer beliebigen Verwendung und damit letztlich die Unüberschaubarkeit und Unkontrollierbarkeit der Verarbeitung aus. Nur solange die für einen bestimmten Zweck erhobenen oder überlassenen Daten lediglich für diesen verarbeitet werden dürfen, läßt sich der Verarbeitungsprozeß offenlegen und nachvollziehen. Der Datenschutz ist insofern eine gezielte Absage an die Datenproliferation.

Ganz in diesem Sinn stellt die Mehrzahl der Datenschutzgesetze fest, daß die aus dem öffentlichen Bereich an Dritte übermittelten Daten ausschließlich für den Zweck genutzt werden dürfen, für den sie überlassen worden sind. In Wirklichkeit wird freilich damit ein allgemeiner Grundsatz des Datenschutzes angesprochen, der zunächst für jede Verarbeitung gilt. Das BDSG muß insofern das Versäumte nachholen und seine Grundsatzbestimmungen um die Zweckbindung ergänzen, unmißverständlich also zum Ausdruck bringen, daß personenbezogene Daten nur für die Zwecke verwendet werden dürfen, für die sie erhoben oder überlassen worden sind.

Wo der Gesetzgeber aber meint, davon abweichen zu müssen, sind Vorkehrungen notwendig, die für eine ähnlich wirksame Einschränkung der Verarbeitung sorgen. Ein Beispiel dafür ist die Übermittlung personenbezogener Daten innerhalb des öffentlichen Bereichs. Hier gibt es in der Tat Argumente, die gegen eine strikt durchgeführte Zweckbindung sprechen. Umgekehrt hat nicht zuletzt die Diskussion über die Grenzen der Amtshilfe, aber auch die Sonderregelung des Sozialgesetzbuches gezeigt, daß ein uneingeschränkter Informationsaustausch im öffentlichen Bereich ebensowenig wie anderswo hingenommen werden kann. Konsequenterweise erkennt daher das neue Melderecht die funktionale Betrachtung der behördlichen Tätigkeit ausdrücklich an. Ihre Bedeutung wird in diesem Bericht an anderer Stelle besonders hervorgehoben (vgl. 4.2). Hier kommt es lediglich darauf an, festzustellen, daß in dem Maße, in dem sich ein funktionaler Behördenbegriff durchsetzt, ein annehmbares Äquivalent für die Zweckbindung geschaffen wird. Der Gesetzgeber muß sich also, gerade wenn es um mögliche Ausnahmen von der Zweckbindung geht, überlegen, ob und in welchem Umfang die durch das Melderechtsrahmengesetz bestätigte Entwicklung vom BDSG weiterzuführen ist.

3.1.2.3
Dateibegriff

Das BDSG hat sich für eine formale Einschränkung seines Anwendungsbereichs entschieden. Seine Vorschriften sind nur so lange anzuwenden, wie personenbezogene Daten in "Dateien" verarbeitet werden. Die Verknüpfung des Datenschutzes mit der Datei ist oft und nachhaltig kritisiert worden. Sie bleibt freilich notwendig, wenn man, wie das BDSG, sich für eine allgemeine Datenschutzregelung entscheidet, die ohne Rücksicht auf das jeweils verwendete Verfahren bei jeder Verarbeitung beachtet werden muß. Dann kann der Gesetzgeber nicht umhin, eine Untergrenze für die Anwendung der Datenschutzbestimmungen anzugeben, die sich an formalen Merkmalen orientiert. Inhaltliche Differenzierungen sind nur dort möglich, wo auf konkrete Konflikte eingegangen wird, es also zu einer bereichsspezifischen Lösung kommt. Wer sich etwa lediglich mit der Verarbeitung von Arbeitnehmerdaten im Unternehmensbereich beschäftigt, muß in der Tat von den Besonderheiten und den Folgen eben dieser Verarbeitung ausgehen und im Hinblick darauf die Verarbeitungsanforderungen festlegen. Auf die Datei kommt es insofern nicht weiter an. Wer dagegen gar nicht erst fragt, um welche Daten es sich handelt und von wem sie für welche Zwecke verarbeitet werden, hat keine andere Möglichkeit, als die Grenzen der beabsichtigten Regelung nach formalen Gesichtspunkten zu ziehen. Kurzum, eine Reform, die am System des BDSG festhält, muß auch die Anknüpfung an die Datei beibehalten.

Die Novellierung braucht sich aber nicht mit der in § 2 Abs. 3 Nr. 3 BDSG enthaltenen Definition der Datei abzufinden. Sie muß vielmehr der fast einhelligen Kritik Rechnung tragen. Zum einen kommt es darauf an, die Verwirrung zu vermeiden, die durch die umständliche Formulierung des BDSG verursacht wird, zum anderen gilt es, die sich abzeichnenden Entwicklungen im Verarbeitungsbereich einzubeziehen, vor allem also auf die sich ständig verfeinernde Verwertung der Datensammlungen, etwa durch assoziative Merkmale, einzugehen. So gesehen, muß von einer "Datei" immer dann gesprochen werden, wenn es sich um eine durch automatisierbare Verfahren auswertbare Sammlung von Daten handelt, oder wenn eine gleichartig aufgebaute Sammlung von Daten vorliegt, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren.

3.1.2.4
Verarbeitungsphasen

Das BDSG bezieht sämtliche Verarbeitungsphasen in seine Regelung ein. Die Erfahrung hat aber gezeigt, daß die BDSG-Vorschriften jedenfalls in zweierlei Hinsicht nicht ausreichen:

3.1.2.4.1
Erhebung

Die gesetzlichen Bestimmungen greifen erst bei der Speicherung ein. Sie lassen insofern die Erhebung außer Betracht. Diese Einschränkung ist bereits während des Gesetzgebungsverfahrens zu recht kritisiert worden. Man

kann die Kritik nicht mit dem Hinweis entkräften, die einmal erhobenen Daten würden ohnehin gespeichert, an der Anwendung des BDSG komme man also doch nicht vorbei. Richtig ist daran soviel: Das BDSG ermöglicht mit seinen Vorschriften wenigstens eine teilweise Korrektur von Erhebungen, die sich mit seinen Grundsätzen nicht vereinbaren lassen. Genau darin liegt freilich der Mangel. Ein wirksamer Schutz fordert mehr als nur nachträgliche Korrekturen; es kommt darauf an, Datenschutzgrundsätzen, wie etwa dem der Erforderlichkeit, bereits im Augenblick der Erhebung Rechnung zu tragen und schon zu diesem Zeitpunkt auf die Situation des Betroffenen und die möglichen Konsequenzen der Informationssammlung Rücksicht zu nehmen. Nicht von ungefähr hat etwa das Betriebsverfassungsrecht (§ 94 BetrVG) die Fragebogen zum Gegenstand seiner Regelung gemacht, sich also auf die Erhebung konzentriert. Eine Einbeziehung der Erhebung muß auch zur Folge haben, daß die unzulässig erhobenen Daten vernichtet werden müssen, ganz gleich im übrigen, ob sie in einer Datei gespeichert worden sind oder nicht.

3.1.2.4.2
Übermittlung - Direktzugriff

3.1.2.4.2.1
Gesetzliche Präzisierung

3.1.2.4.2.1.1
Bisheriger Rechtszustand

Bereits im 9. Tätigkeitsbericht (vgl. 2.1) war ausführlich auf die Gefahren hingewiesen worden, die ein Direktanschluß mit sich bringt (vgl. dazu auch oben 2.3.1). Die Übermittlungsvorschriften des BDSG reichen nicht aus; eine Sonderregelung ist, wie auch die Diskussion im Hessischen Landtag und die Empfehlung des Parlaments gezeigt haben, unerläßlich. Sie muß auf die spezifische, mit dem Direktanschluß verbundene Form des Zugriffs zugeschnitten sein und über die Verarbeitungsbedingungen hinaus auch Maßnahmen der Datensicherung im organisatorischen und technischen Bereich enthalten.

Ausgangspunkt einer rechtlichen Lösung des Problems müssen die an der Einzelfallübermittlung ausgerichteten, geltenden Vorschriften sein. Sie unterscheiden je nach der Zuordnung des Empfängers eine Übermittlung innerhalb des öffentlichen Bereichs (§ 10 BDSG) und eine Übermittlung aus dem öffentlichen in den privaten Bereich (§ 11 BDSG). Eine Übermittlung ist innerhalb des öffentlichen Bereichs zulässig, wenn sie "zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist" (§ 10 BDSG). Für beide Alternativen gilt damit das Erforderlichkeitsprinzip. Es enthält zwei Aspekte: zum einen, ob die geforderte Datenübermittlung überhaupt geeignet ist, die jeweilige Aufgabe zu erfüllen, und zum andern, ob sie den geringstmöglichen Eingriff im Vergleich zu anderen Mitteln darstellt (Verhältnismäßigkeit). Hieraus folgt, daß strenge Anforderungen an die Auslegung des Begriffs "erforderlich" zu stellen sind. Kurzum: Eine Übermittlung ist nur dann "erforderlich", wenn der angestrebte Zweck nicht mit anderen Mitteln zu erreichen ist.

3.1.2.4.2.1.2
Kontrolle der Voraussetzungen der Übermittlung

An jedem Übermittlungsvorgang sind zwei Stellen beteiligt. Damit stellt sich die Frage, wer prüft, ob die Übermittlung erforderlich ist. Nähme man nach § 7 Abs. 2 des Verwaltungsverfahrensgesetzes des Bundes die allgemeine Amtshilferegelung zum Maßstab, trüge die ersuchende (abrufende) Behörde die Verantwortung für die Rechtmäßigkeit der über die Übermittlung ermöglichten Verwaltungsmaßnahme; die ersuchte Behörde wäre allein für die Durchführung der Übermittlung verantwortlich. So könnte sich die Behörde, aus deren Beständen die Daten übermittelt werden, darauf beschränken, festzustellen, ob die anfragende Stelle allgemein für die rechtmäßige Erfüllung der genannten Verwaltungsaufgaben zuständig ist. Dies hätte zur Konsequenz, daß die ersuchte Behörde weitgehend den Einfluß auf das Schicksal ihrer Daten verlieren würde - ein angesichts der Strafvorschriften von § 41 Abs. 1 Nr. 1 BDSG bedenkliches Ergebnis. Sie wäre dann praktisch kaum mehr verantwortlich für die Rechtmäßigkeit der Übermittlung.

Aus diesem Grunde kann sich die Prüfung der Erforderlichkeit im Datenschutzrecht nicht nach den Amtshilfevorschriften richten. Will die ersuchte Behörde auch im Bereich der Datenübermittlung "Herr ihrer Daten" sein, so muß sich ihre Prüfung auch darauf erstrecken, ob Daten der zu übermittelnden Art, ja ob alle angeforderten Daten im einzelnen zur Aufgabenerfüllung der ersuchenden Behörde erforderlich sind. Dieses umfassende Prüfungsrecht - dem eine ebenso umfassende Prüfungspflicht entspricht - kommt natürlich dort nur eingeschränkt zur Anwendung, wo Übermittlungen des gleichen Typs sich wiederholen oder einem klaren Schema folgen. Ein Höchstmaß an Datenschutz ist insofern nur dann gewährleistet, wenn zwischen dem Verfügungsrecht der ersuchten Stelle über ihre eigenen Daten und der Verantwortung der Empfängerstelle für die mit der Übermittlung verfolgte Aufgabenerfüllung eine "praktische Konkordanz" gefunden wird. Konkret heißt das, daß die anfragende Behörde - für die

Sonderfälle etwa des Sicherheits- und Sozialbereichs kann dies nur mit Einschränkungen gelten - der ersuchten Behörde so viele Informationen zur Verfügung zu stellen hat, daß diese mindestens eine Plausibilitätsprüfung durchführen kann, die sich auf die Erforderlichkeit der Übermittlung überhaupt sowie die angefragten Daten nach Menge und Qualität erstreckt.

3.1.2.4.2.1.3
Direktzugriff anstelle von Massen- oder Einzelübermittlungen

Der Direktzugriff kommt in zwei Fällen zur Anwendung, die rechtlich unterschiedlich gewertet werden müssen. Einmal ersetzt er die traditionelle **Massen**übermittlung von Daten, die darauf beruht, daß die empfangende Stelle in einer Vielzahl gleichgelagerter Fälle einen festgelegten Datensatz benötigt. So übermittelt etwa die Kraftfahrzeugzulassungsstelle dem Finanzamt in jedem Fall einer Änderung die Halterdaten mit einem bestimmten Datensatz, der zur Festsetzung der Kfz-Steuer benötigt wird. Massenübermittlungen dieser Art sind dadurch gekennzeichnet, daß jedes einzelne Datum zur Aufgabenerfüllung der empfangenden Stelle "erforderlich" ist und die Prüfung dieser Erforderlichkeit pauschal vor der Einrichtung des "Übermittlungsstroms" erfolgt. Soweit das Direktzugriffsverfahren an die Stelle einer regelmäßigen Massenübermittlung tritt, steht es nicht im Widerspruch zu den derzeit geltenden Gesetzen.

Anders zu bewerten ist hingegen der Fall, in dem die traditionelle **Einzelfall**übermittlung durch eine Direktanbindung ersetzt wird. Hier wird zur Arbeitserleichterung "auf Vorrat" ein bestimmter Datensatz zur Verfügung gestellt. Die darin enthaltenen Einzeldaten **können** zur Aufgabenerfüllung der Empfängerbehörde benötigt werden. Ob und wann dies der Fall sein wird, weiß zum Zeitpunkt der Einrichtung des Direktzugriffsverfahrens niemand. In der Regel wird auch nur ein kleiner Teil der auf diese Weise übermittelten Daten tatsächlich von der abfragenden Stelle benötigt. Typischer Fall ist die Anbindung der Polizei an Dateien anderer Behörden (Einwohnermeldeämter, Kfz-Zulassungsstellen). Noch einmal: Der Einsatz des Direktzugriffs - auch in dem nach der derzeitigen Rechtslage unzulässigen Bereich - bietet administrative Vorteile. Rechtlich gesehen wäre er dann unbedenklich, wenn dieser besonderen technischen Anordnung eine normative Struktur zugrunde gelegt werden könnte, die eine vergleichbare Einschränkung und Kontrolle wie bei der traditionellen Einzelfallübermittlung zuließe.

3.1.2.4.2.1.4
Vorgaben aus dem Melderechtsrahmengesetz

Die Novellierung der Datenschutzgesetze könnte dabei teilweise auf eine bereits geltende Rechtsvorschrift zurückgreifen: Das Melderechtsrahmengesetz unterscheidet zwischen der **Einzelfall**übermittlung (§ 18 Abs. 1 - 3) und der **regelmäßigen** Datenübermittlung (§ 18 Abs. 4). Die Regelung der Einzelfallübermittlung entspricht in ihrer Struktur den Übermittlungsvorschriften der Datenschutzgesetze. Für regelmäßige Datenübermittlungen verlangt das Gesetz eine besondere Festlegung im Bundes-oder Landesrecht "unter Feststellung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten". Dies ist von erheblicher Bedeutung, weil mit dieser Vorschrift nicht nur traditionelle regelmäßige Massenübermittlungen geregelt werden sollten, sondern auch Direktzugriffe auf das Melderegister der Gemeinden. - Nebenbei gesagt: Die äußerst detaillierte Regelung der Erforderlichkeitsprüfung bei der Einzelfallübermittlung an andere Behörden in § 18 Abs. 1 - 3 MRRG weist noch einmal deutlich auf die datenschutzrechtliche Bedeutung dieser Prüfung durch die ersuchte Behörde sowie ihre abweichende Struktur im Vergleich zu den Amtshilferegeln hin.

Rechtstechnisch bedeutet die Regelung in § 18 Abs. 4 MRRG, daß **der Gesetz- bzw. Verordnungsgeber im voraus** die Erforderlichkeitsprüfung vornimmt. Dieses Verfahren erscheint ausreichend, soweit **Massen**übermittlungen betroffen sind. So werden sowohl die ersuchte als auch die ersuchende Behörde entlastet; die Übermittlungen können ohne weitere rechtliche Prüfung im Einzelfall durchgeführt werden. Soweit der Direktzugriff allerdings **Einzelfall**übermittlungen ersetzt, ist die Regelung des § 18 Abs. 4 unzureichend und müßte ergänzt werden. Da die Erforderlichkeitsprüfung sich nicht auf den Direktzugriff als solchen beziehen kann - das Verfahren an sich wird kaum jemals erforderlich sein; es ist allenfalls schneller und genauer -, muß sie sich an den konkreten Abruf im Einzelfall halten. Nach der bisherigen Rechtslage gelten die bereitstehenden Daten ja bereits als übermittelt und stehen damit - rechtlich gesehen - dem Zugriff der abfragenden Behörde ohne Einschränkung zur Verfügung. Der Abruf von Daten darf jedoch nur dann zulässig sein, wenn die Daten konkret im Zeitpunkt des Abrufs zur rechtmäßigen Aufgabenerfüllung der abrufenden Stelle erforderlich sind. Dieser Stelle muß deshalb die Rechtspflicht auferlegt werden, diese Voraussetzungen im Einzelfall zu prüfen. Eine Protokollierung des Abrufs ist vorzusehen, um kontrollieren zu können, ob der Zugriff im Einzelfall im Rahmen dieser Schranken erfolgt ist.

Das Direktzugriffsverfahren erleichtert den Zugang zu den Daten des Bürgers im Vergleich mit der traditionellen Übermittlung erheblich. Diese Überlegung ist Grundlage der Entscheidung, die Einrichtung von Direktzugriffsverfahren nur dort zuzulassen, wo spezielle administrative Belange gegenüber den Interessen des einzelnen Bürgers Vorrang haben. Ein Direktzugriff der öffentlich-rechtlichen Religionsgesellschaften oder von Stellen im nichtöffentlichen Bereich auf Dateien öffentlicher Stellen sollte deshalb ausgeschlossen werden.

3.1.2.4.2.2
Regelungsvorschlag

Im einzelnen wären die §§ 10 und 11 BDSG wie folgt neu zu fassen (die neu formulierten Teile dieser Vorschriften sind fett gedruckt):

§ 10
(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.

(2) Regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen sind zulässig, soweit dies durch Bundesrecht unter Feststellung des Anlasses und des Zweckes der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Der Abruf von Daten im Verfahren des Direktzugriffs ist zulässig, soweit die Kenntnis der Daten zur rechtmäßigen Aufgabenerfüllung der abrufenden Stelle erforderlich ist. Die abrufende Stelle prüft die Voraussetzungen im Einzelfall. Der Abruf im Einzelfall ist aufzuzeichnen. Näheres bestimmt die nach Satz 1 zu erlassende Rechtsvorschrift.

(3) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1, Satz 3) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß der Empfänger die Daten zur Erfüllung des gleichen Zweckes benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

(4) Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an Behörden und sonstige öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

Die regelmäßige Übermittlung personenbezogener Daten von öffentlichen Stellen an Stellen der öffentlich-rechtlichen Religionsgesellschaften im Verfahren des Direktzugriffs ist nicht zulässig.

§ 11
(1) Die Übermittlung personenbezogener Daten an Personen und an andere Stellen als die in § 10 bezeichneten ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

(2) Die regelmäßige Übermittlung personenbezogener Daten von öffentlichen Stellen an Stellen außerhalb des öffentlichen Bereiches im Verfahren des Direktzugriffs ist nicht zulässig.

(3) Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1, Satz 3) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person übermitteln dürfte.

(4) Für die Übermittlung an Behörden und sonstige Stellen außerhalb des Geltungsbereiches dieses Gesetzes sowie an über- und zwischenstaatliche Stellen finden die Sätze 1 und 2 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen Anwendung.

Die Einrichtung von Direktzugriffsverfahren im öffentlichen Bereich (§§ 10, 11 BDSG) setzt besondere Maßnahmen der Datensicherung voraus. § 6 BDSG ist deshalb entsprechend zu ergänzen. Dabei sollten folgende Forderungen berücksichtigt werden:

1. Die technische Einrichtung eines Direktzugriffsverfahrens bedarf der Genehmigung durch die zuständige oberste Bundesbehörde.

2. Die Genehmigung bezieht sich auf die Geräteausstattung (Hardware), die anzuwendenden Programme (Software) sowie Maßnahmen der Datensicherung.

3. Der Bundesbeauftragte für den Datenschutz erhält ein Mitwirkungsrecht (Anhörung) im Genehmigungsverfahren.

3.1.2.4.3
Wissenschaftliche Forschung

Besondere Probleme stellen sich bei der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung. Wohlgemerkt, es geht nicht darum, die Forschung von der Verpflichtung auszunehmen, den Anforderungen des Datenschutzes Rechnung zu tragen. Zur Debatte steht allein eine Regelung, die auf die Erwartungen der Forschung eingeht, auch und gerade mit Hilfe personenbezogener Daten arbeiten zu können, ohne zugleich den Datenschutz in Frage zu stellen. Das BDSG vermeidet es, Stellung zu nehmen. Die Landesdatenschutzgesetze versuchen dagegen, wie sich an § 15 HDSG zeigt, eine Lösung zu finden. Die Diskrepanz überrascht freilich nicht. Die Regelung von Fragen, die mit der wissenschaftlichen Forschung zusammenhängen, gehört zum Kompetenzbereich der Länder. Konsequenterweise ist deshalb in Hessen eine Vielzahl von Einzelproblemen geregelt worden.

Bei einer Novellierung des BDSG gilt es deshalb, sich von vornherein auf die Aspekte zu beschränken, die aus der Perspektive eines Bundesgesetzes allein in Betracht kommen, genauer, auf die Fragen der Übermittlung personenbezogener Daten aus dem Bereich der Bundesverwaltung an wissenschaftliche Institutionen für Forschungszwecke. Die Übermittlung darf dabei immer nur für ein bestimmtes Forschungsvorhaben erfolgen und muß grundsätzlich von der Einwilligung des Betroffenen abhängig sein. Von der Einwilligung ist lediglich dann abzusehen, wenn der Forschungszweck anders nicht erreicht werden kann und seine Verwirklichung schutzwürdige Belange des Betroffenen nicht gefährdet. Darüber hinaus muß klargestellt werden, daß jede weitere Übermittlung und jede zusätzliche Nutzung ebenfalls der Einwilligung des Betroffenen bedarf. Die Daten müssen ferner so bald wie möglich anonymisiert werden. Die gesetzliche Regelung muß schließlich den Zugriff Dritter auf die ausschließlich zu Forschungszwecken überlassene Information ausdrücklich unterbinden.

3.1.2.5
Rechte des Betroffenen

Das BDSG räumt genauso wie die Landesdatenschutzgesetze dem Betroffenen eine Reihe von Rechten ein. Sie ermöglichen es ihm, eine korrekte Verarbeitung zu verlangen, Informationsverzerrungen also zu unterbinden. Der Betroffene kann aber seine Rechte nur auf der Grundlage einer zuverlässigen und zutreffenden Kenntnis der Verarbeitung ausüben. Das BDSG gewährt ihm deshalb ein Auskunftsrecht. So richtig diese Entscheidung auch ist, so wenig sind die Nachteile der gesetzlichen Regelung zu übersehen:

3.1.2.5.1
Auskunftsgebühr

Die Rechte des Betroffenen riskieren solange illusorisch zu bleiben, wie die Auskunft an eine Gebühr geknüpft ist. Die große Zahl der speichernden Stellen sowohl im öffentlichen als auch im privaten Bereich macht eine noch so geringe Gebühr für jede einzelne Auskunft zu einer für den Betroffenen in aller Regel unzumutbaren Belastung. Der hessische Gesetzgeber hat daraus die einzig mögliche Konsequenz gezogen: die Gebührenpflicht ist abgeschafft. Andere Länder sind diesem Beispiel mittlerweile gefolgt. Das BDSG muß dieser Entwicklung angepaßt werden, und zwar nicht nur für den öffentlichen Bereich. Die Erfahrungen der Aufsichtsbehörden haben nur zu gut gezeigt, wie sehr die Gebühren immer wieder dazu genutzt worden sind, um dem Betroffenen die Information über die Verarbeitung seiner Daten zu verweigern oder zumindest beträchtlich zu erschweren. Die Intervention der Aufsichtsbehörden hat dazu geführt, daß auch im privaten Bereich weitgehend auf Gebühren verzichtet worden ist. Wenn der Gesetzgeber den Betroffenen ernsthaft an der Kontrolle der Verarbeitung seiner Daten beteiligen will, geht es nicht an, Zugangsbedingungen zu formulieren, die den Zugang versperren, statt ihn zu öffnen.

3.1.2.5.2
Benachrichtigungspflicht

Das Auskunftsrecht darf freilich nicht überschätzt werden. Für den Betroffenen ist es, wie sich an den Erfahrungen der Datenschutzbeauftragten und der Aufsichtsbehörden ablesen läßt, keineswegs selbstverständlich, Auskunft zu verlangen. Kaum verwunderlich, wenn man bedenkt, daß der Betroffene zumeist von der Verarbeitung seiner Daten nichts oder bestenfalls sehr wenig weiß. Ihm deshalb Rechte ohne einen ebenso regelmäßigen wie verständlichen Überblick über die ihn betreffende Verarbeitung zu gewähren, hat wenig Sinn. Vorschriften wie § 12 BDSG sind insofern verfehlt; Amtsblätter gehören nun einmal nicht zur Alltagslektüre des einzelnen. Aber auch die für den privaten Bereich vorgesehene Benachrichtigung bei der erstmaligen Speicherung (§ 26 Abs. 1) oder Übermittlung (§ 34 Abs. 1) hilft nicht weiter. Bedenklich sind schon die weitreichenden Ausnahmen. Ganz abgesehen davon ist aus der Perspektive des Betroffenen eine kontinuierliche Information erforderlich. Nur dann kann er sich wirklich ein Bild von der Verarbeitung machen und von sich aus entscheiden, ob und gegenüber welcher speichernden Stelle Auskunfts- und Korrekturrechte möglicherweise einen Sinn haben.

Der Gesetzgeber muß sich deshalb mit der Frage auseinandersetzen, inwieweit ein wirksamer Datenschutz nicht eine regelmäßige und gezielte Benachrichtigung des Betroffenen voraussetzt, die ihm unmittelbar Kenntnis von der Verarbeitung verschafft. Wohlgemerkt, es geht nicht darum, ihn zu informieren, was im einzelnen verarbeitet wird, sondern lediglich, daß eine Verarbeitung stattfindet. Ähnliche Überlegungen haben bei der Verarbeitung von Arbeitnehmerdaten zu ersten Versuchen einer kontinuierlichen Benachrichtigung geführt. Diesen Weg gilt es auch im BDSG zu beschreiten.

3.1.2.5.3
Berichtigung

Das BDSG gewährt dem Betroffenen ein Berichtigungsrecht (§ 4 Nr. 2). Es bleibt freilich auf halbem Wege stehen. Sicher ist es für den Betroffenen wichtig, daß die speichernde Stelle die jeweils erforderlichen Korrekturen vornimmt. Doch spätestens an den Übermittlungsvorschriften des BDSG zeigt sich, daß einer der weitreichendsten Aspekte der Verarbeitung personenbezogener Daten ihre Weitergabe an Dritte ist. Gerade im Hinblick darauf hat die Diskussion über den Datenschutz begonnen, und genau diese Informationsverbreitung hat lange Zeit fast ausschließlich im Mittelpunkt der Überlegungen des Gesetzgebers gestanden. Dann aber kann und darf es nicht ausreichen, dem Betroffenen ein Berichtigungsrecht zuzugestehen, das nicht mehr bewirkt als Korrekturen bei der speichernden Stelle. Sie muß vielmehr verpflichtet werden, alle regelmäßigen, aber auch alle gespeicherten Informationsempfänger unverzüglich über die Berichtigung zu benachrichtigen.

3.1.2.6
Kontrollrechte der Aufsichtsbehörden

Das BDSG hat sich auch im privaten Bereich für eine Fremdkontrolle entschieden. Doch die lange Zeit vorherrschende Vorstellung, daß man sich eigentlich mit einer Selbstkontrolle zufriedengeben sollte, ist nicht ohne Auswirkungen geblieben. Das zeigt sich schon an den unterschiedlichen Kontrollvorstellungen, je nachdem ob die personenbezogenen Daten nur für eigene Zwecke oder geschäftsmäßig für fremde Zwecke verarbeitet werden. Im ersten Fall macht das Gesetz (§ 30) die Kontrolle durch die Aufsichtsbehörde von einem konkreten, vom Betroffenen darzulegenden Anlaß abhängig, im zweiten spricht es sich (§ 40) für eine regelmäßige Überwachung aus. Diese Unterscheidung ist weder vom Umfang noch von der Bedeutung der Verarbeitung her gerechtfertigt. Sicher, die geschäftsmäßige Verarbeitung scheint auf den ersten Blick sehr viel weiterreichende Konsequenzen für den Betroffenen zu haben und damit auch für eine schärfere Kontrolle zu sprechen. Wie wenig zutreffend solche Überlegungen freilich sind, zeigt sich am Beispiel der Arbeitnehmerdaten. Sie gehören zu den am meisten verarbeiteten personenbezogenen Angaben. Wahrscheinlich in keinem anderen Fall ist die Verflechtung der verschiedensten Institutionen vom Unternehmen selbst über Versicherungen und Krankenkassen bis hin zu staatlichen Instanzen so offenkundig.

Nicht zuletzt deshalb geht es nicht an, die Kontrolle zurückzunehmen. Der Gesetzgeber muß vielmehr die im BDSG getroffene Unterscheidung aufgeben und sich für eine einheitliche, die ständige Überwachung durch die Aufsichtsbehörde ermöglichende Regelung aussprechen. Der Aufsichtsbehörde darf auf keinen Fall weiterhin das Recht versagt werden, auch dort von sich aus zu kontrollieren, wo die personenbezogenen Daten nur für eigene Zwecke verarbeitet werden.

Ebenso wichtig ist es, die Aufsichtsbehörde mit Eingriffsrechten auszustatten. Die §§ 30 und 40 BDSG weisen ihr, genaugenommen, letzlich nur die Funktion eines Beobachters und bestenfalls Beraters zu. Selbst in den Fällen, in denen nach § 39 BDSG eine Meldepflicht besteht, kann die Aufsichtsbehörde auch dann nicht eingreifen und erkennbare Verstöße gegen den Datenschutz unmittelbar unterbinden, wenn sie aus der Meldung eindeutig zu erkennen sind. Zudem braucht sich die speichernde Stelle keineswegs nach den Vorschlägen der Aufsichtsbehörde zu richten. Als Druckmittel steht ihr allenfalls die Geldbuße nach § 42 BDSG zur Verfügung. Ein wirksamer Datenschutz erfordert aber mehr als nur die späte und in ihren Konsequenzen für die weitere Verarbeitung keineswegs verläßliche Reaktion in Form einer Geldbuße. Nicht von ungefähr haben die Aufsichtsbehörden dann den Verarbeitungsprozeß wirklich beeinflußt, wenn sie sich, wie etwa bei Versicherungsunternehmen, an spezielle Aufsichtsinstanzen wenden konnten, die ihrerseits mit Eingriffsrechten ausgestattet sind. Erst der Druck dieser Instanzen hat die im Interesse des Datenschutzes notwendigen Korrekturen bewirkt, wie etwa das Beispiel der Einwilligung bei Versicherungsverträgen zeigt.

Die Aufsichtsbehörde muß deshalb entgegen der bisherigen Regelung die Möglichkeit erhalten, Maßnahmen zum Vollzug von Datensicherungsvorkehrungen anzuordnen, Verfahren zu verbieten, die gegen die jeweils erforderlichen technisch-organisatorischen Sicherungsvorkehrungen verstoßen und schließlich die Verarbeitung ganz oder teilweise zu untersagen, wenn der Datenschutz nicht sicherzustellen ist.

Darüberhinaus muß klargestellt werden, daß es zu den Aufgaben der Aufsichtsbehörde gehört, den Betroffenen über das Ergebnis der Kontrolle auch dort zu unterrichten, wo sie nicht durch ihn ausgelöst wird. Die Fremdkontrolle rechtfertigt sich nicht zuletzt aus der Überlegung, daß der Betroffene selbst zumeist gar nicht in der Lage ist,

den Umfang der Verarbeitung seiner Daten nachzuvollziehen, geschweige denn, den Verarbeitungsprozeß zu überschauen. Die Aufsichtsbehörde handelt deshalb auch und gerade für ihn. Ihre Erkenntnisse sind insofern die für eine Ausübung seiner Rechte unentbehrliche Grundlage; er ist daher auf eine ebenso rechtzeitige wie vollständige Unterrichtung angewiesen.

Das Gesetz sollte schließlich eine jährliche Berichtspflicht vorsehen, mit dem Ziel, die konkreten Erfahrungen der Aufsichtsbehörden zum Anlaß zu nehmen, um die Öffentlichkeit sowie den Gesetzgeber auf Sonderaspekte und Entwicklungstendenzen der Verarbeitung personenbezogener Daten im privaten Bereich aufmerksam zu machen. Nur auf diesem Weg läßt sich gegen die in diesem Bericht bereits erwähnte ungleichgewichtige Betrachtung des Datenschutzes wirksam angehen. Noch einmal: Die Verarbeitungsgefahren sind keineswegs ausschließliche Begleiterscheinung der Aktivität staatlicher Instanzen. Zu Recht hat der Gesetzgeber sowohl den öffentlichen als auch den privaten Bereich in seine Regelung einbezogen. Er muß nur die Konsequenz aus dieser Entscheidung ziehen und für eine kontinuierliche Information über beide Bereiche sorgen.

3.1.2.7
Datenschutzbeauftragte im privaten Bereich

Das BDSG sieht im privaten Bereich neben der Fremdkontrolle eine interne Überwachung vor. Die speichernde Stelle muß unter bestimmten, im Gesetz näher geregelten Umständen einen Beauftragten für den Datenschutz bestellen (§§ 28, 38). Diese Entscheidung ist wiederholt kritisiert worden. Die Erfahrung hat freilich gezeigt, daß der Datenschutz entgegen mancher Befürchtung davon durchaus profitiert. Es liegt sowohl im Interesse des Betroffenen als auch der speichernden Stelle selbst, einen Ansprechpartner zu haben, der über die notwendige Sachkunde hinaus die Unternehmensorganisation kennt und deshalb beurteilen kann, wie die Datenschutzanforderungen im Bereich der speichernden Stelle in einer den Erwartungen des Gesetzes entsprechenden Weise realisiert werden können. Verständlicherweise haben sich mittlerweile auch in weiten Teilen der öffentlichen Verwaltung ähnliche Vorstellungen durchgesetzt.

Die Erfahrung zeigt aber auch, daß der Beauftragte für den Datenschutz von Anfang an Konflikten ausgesetzt ist, die seine Tätigkeit erschweren und damit gerade jene vom Gesetz angestrebte Überwachung des Datenschutzes (§ 29) in Frage stellen. So wenig deshalb an der Notwendigkeit gezweifelt werden kann, die Entscheidung des Gesetzgebers für die Bestellung eines Beauftragten aufrechtzuerhalten, so sehr kommt es darauf an, Korrekturen vorzunehmen, die in Kenntnis der Konflikte die Position des Beauftragten stärken. Dazu zählt zunächst die ausdrückliche gesetzliche Verankerung seiner Schweigepflicht. Solange es daran fehlt, sieht sich der Beauftragte immer wieder dem Verdacht ausgesetzt, alle Informationen, die er im Rahmen seiner Tätigkeit erhält, an die speichernde Stelle weiterzugeben. Sie ist für den Datenschutz verantwortlich, sie entscheidet über seine Bestellung, und von ihr ist er abhängig. Die Schweigepflicht ist eine notwendige Informationsbarriere, die Mißtrauen abbaut und zugleich jene Trennung zwischen der speichernden Stelle und dem Beauftragten unterstreicht, die das Gesetz in § 28 durch die Weisungsfreiheit und das Benachteiligungsverbot ausdrücklich anerkennt. Darüberhinaus muß für den Datenschutzbeauftragten ein besonderer Kündigungsschutz vorgesehen werden. Sein Arbeitsverhältnis darf nur aus wichtigem Grund gekündigt werden (§ 626 BGB). Der speichernden Stelle muß infolgedessen die Möglichkeit genommen werden, durch eine relativ leichte Auflösung des Arbeitsverhältnisses die ohnehin bestehende Abhängigkeit zu verstärken.

Schließlich gilt es, die Bestellung des Beauftragten an die Mitbestimmung des Betriebsrats zu knüpfen. Der Beauftragte ist seiner ganzen Stellung nach eben kein "verlängerter Arm" des Arbeitgebers. Er hat in erster Linie für die Interessen aller von der Verarbeitung Betroffenen zu sorgen, und zwar auch und gerade dann, wenn sie sich nicht mit den Erwartungen der speichernden Stelle decken. Kaum jemand anderes ist aber so von der Verarbeitung betroffen wie die Arbeitnehmer. Zudem kann kein Beauftragter seine Aufgabe wirklich erfüllen, ohne mit dem Betriebsrat ständig zu kooperieren. Das gilt für die Kontrolle der Verarbeitung von Arbeitnehmerdaten ebenso wie für die in § 29 BDSG vorgesehene Schulungs- und Beratungsfunktion. Gerade deshalb kommt es ganz besonders darauf an, die Entscheidung über die Bestellung in einer Weise zu treffen, die den Arbeitnehmern nicht das Gefühl vermittelt, daß an ihnen vorbei eine neue, vom Arbeitgeber gesteuerte Kontrollinstanz geschaffen wird. Der Weg dazu ist die Mitbestimmung des Betriebsrats.

3.1.2.8
Schadensersatz

Das BDSG sieht bei Verstößen gegen die Datenschutzvorschriften Strafen (§ 41) und Geldbußen (§ 42) vor. Die Landesdatenschutzgesetze gehen weiter: Sie haben sich, wie etwa § 8 Abs. 2 HDSG zeigt, für einen Schadensersatz ausgesprochen. Das BDSG hat freilich, genaugenommen, die Entscheidung offengelassen. Der Gesetzgeber meinte zunächst einmal abwarten zu müssen, ob die allgemeinen Schadensersatzvorschriften nicht ausreichten, wollte also wenigstens vorerst eine Sonderregelung vermeiden. Die Zurückhaltung kann aber leicht zu falschen Schlußfolgerungen verleiten. Allzu nahe liegt in der Tat die Annahme, der Gesetzgeber habe mit dem BDSG eine abschließende Regelung der Verarbeitung personenbezogener Daten getroffen und deshalb auch die möglichen Sanktionen bewußt beschränkt. Für eine Anwendung etwa der bürgerlichrechtlichen Schadensersatzbestimmungen gebe es insofern keinen Raum mehr.

Man kann über den Wert einer Schadensersatzvorschrift durchaus streiten. Aus der Perspektive des Betroffenen ist es weitaus wichtiger, den Verarbeitungsprozeß von Anfang an an Voraussetzungen zu binden, die Gefährdungen ausschließen. Nachträgliche Korrekturen können ihm niemals das Maß an Schutz bringen, das eine gezielte, gesetzlich abgesicherte Einschränkung der Verarbeitung ermöglicht. Schadensersatzvorschriften sind dennoch, schon wegen ihrer Präventivfunktion, nicht überflüssig. Darüber hinaus können sie dort, wo es wirklich zu einem Schaden kommt, dem Betroffenen jedenfalls einen gewissen Ausgleich bieten. Allerdings unter drei Voraussetzungen: der Schadensersatz muß verschuldensunabhängig sein, immaterielle Schäden umfassen und darf nicht auf eine Höchstsumme begrenzt sein.

Konsequenterweise hat sich bei den Landesdatenschutzgesetzen der Verzicht auf eine verschuldensabhängige Haftung weitgehend durchgesetzt. Dagegen beschränken die Landesgesetze den Ersatz auf materielle Schäden. Die Ersatzpflicht büßt aber damit ihre Ausgleichsfunktion ein. Schäden, die durch eine rechtswidrige Verarbeitung entstehen, lassen sich durchaus mit den Schäden aus Pressedelikten vergleichen. Hier wie dort spielen die immateriellen Konsequenzen aus der Verbreitung unzutreffender oder unzulässiger Informationen eine entscheidende Rolle. Hier wie dort kommt es deshalb darauf an, den typischen Folgeschäden Rechnung zu tragen, sich also an der Situation des Betroffenen zu orientieren und nicht den Schädiger zu begünstigen. Nichts anderes gilt für die Frage, ob eine Höchstsumme vorgeschrieben werden muß. Der Gesetzgeber hat sich auch sonst nicht durchweg für eine Höchstsumme entschieden. Es gibt deshalb keinen verbindlichen Grundsatz, der die verschuldensunabhängige Haftung an eine Höchstsumme koppelt. Maßgeblich kann vielmehr allein die konkrete, jeweils zu regelnde Situation sein. Gerade im Hinblick auf die besondere Bedeutung des Datenschutzes und die schwerwiegenden Auswirkungen, die eine rechtswidrige Verarbeitung haben kann, erscheint es aber richtig, von einer Beschränkung der Schadensersatzsumme abzusehen. Die Sanktion muß den Wert widerspiegeln, den der Gesetzgeber der Verpflichtung einräumt, die Verarbeitung personenbezogener Daten nur unter bestimmten, von ihm selbst festgelegten Voraussetzungen vorzunehmen.

3.2
Archivgesetz

Die öffentliche Diskussion über das Verhältnis von Datenschutz und Zugang zu Archiven ist nicht zuletzt durch den "Schinderhannes-Fall" ausgelöst worden. Der Datenschutz - so hieß es in der Presse - verhindere die Erforschung der Familienverhältnisse des bekannten rheinischen Räubers. Rheinland-pfälzische Standesbeamte hatten unter Berufung auf eine Ausführungsverordnung zum Personenstandsgesetz einigen historisch Interessierten den Einblick in die immerhin fast 200 Jahre alten Familienstandsdokumente vorenthalten. Zwar hat niemand der Beteiligten sich auf das Datenschutzgesetz berufen, das auch nur für lebende Personen seine Schutzwirkung entfaltet: das Etikett "Datenschutz" für die Ausführungsverordnung zum Personenstandsgesetz war jedoch dennoch schnell zur Hand.

Überhaupt überall wo der Zugang zu historischen Dokumenten verwehrt wird, ist von einer Behinderung durch den Datenschutz die Rede. Ein Grund dafür ist, daß die jeweilige öffentliche Stelle sich oft in Verkennung des Anwendungsbereichs des Datenschutzgesetzes fälschlicherweise darauf beruft, ein weiterer, daß durch die Diskussion um den Datenschutz andere, bisher wenig beachtete Geheimhaltungsbestimmungen aktualisiert und dann einfach dem Datenschutz zugerechnet werden.

Zwei Aspekte stehen im Vordergrund aller Überlegungen:
der Schutz der Persönlichkeitsrechte Betroffener in staatlichen und privaten Archiven einerseits und die Verfügbarkeit historischer Informationen für die wissenschaftliche Forschung andererseits. Resolutionen des Verbands der Historiker Deutschlands, der Fachgruppe Presse-, Rundfunk- und Filmarchivare im Verein Deutscher Archivare sowie namhafte Zeithistoriker in der Bundesrepublik forderten gesetzliche Regelungen zur Sicherung der zukünftigen historischen Forschung und für die archivische Arbeit.

Konkrete Fälle aus der Praxis erweisen die Notwendigkeit gesetzgeberischer Initiativen. Hierbei steht besonders die zeithistorische Forschung über den Nationalsozialismus und die unmittelbare Nachkriegsgeschichte vor besonderen Schwierigkeiten. Die Auseinandersetzung um die Publikation der sog. "Judendokumentation" der Stadt Königstein zeigt in aller Deutlichkeit, welche Konflikte hier auftreten können. Die Geschichte der Juden in einem Ort ist immer auch die Geschichte ihrer Feinde und Freunde, die der Indifferenten und Mitläufer, die der Verfolger, der Denunzianten und der nationalsozialistischen Aktivisten. Die Dokumentation, wäre sie veröffentlicht worden, hätte Ortsgeschichte aktualisiert, vielleicht auch verheilte Narben wieder aufbrechen lassen. Verdrängtes Tun mancher Überlebenden wäre in Erinnerung gerufen, vielleicht aber auch voreiliger Etikettierung das Feld eröffnet worden. Es sind ganz wesentliche Fragen des Umgangs mit der nationalsozialistischen Vergangenheit, die hier berührt werden. Unbeantwortet bleibt, wie sich der Informationsanspruch vor allem der nachfolgenden Generation zu dem Schutz von Betroffenen, seien sie Opfer oder Verfolger, verhält. Der Datenschutz ist kein Lösungstopos für diese Problematik. Der Gesetzgeber hat sich bisher zu diesen Fragen nicht geäußert.

Wie sehr dies notwendig wäre, zeigt auch folgender Fall:
Die Landesregierung verwehrt bisher jedem Forscher Einblick in die ca. dreieinhalb Millionen Spruchkammerakten der Entnazifizierung in Hessen. Große Untersuchungen über die Entnazifizierung, wie sie aus Bayern oder Nordrhein-Westfalen vorliegen, sind in Hessen also nicht möglich, ebensowenig eine Nutzung dieser Akten als Quellen für eine Strukturgeschichte der regionalen NSDAP-Gliederungen. Dieser Sachverhalt wurde aufgrund einer Eingabe aktuell, mit der sich Ende 1981 der Kulturpolitische Ausschuß des Landtags befaßt hat:

Die Gesamthochschule Kassel (GHK) betreibt das interdisziplinäre Forschungsvorhaben "Kassel unter dem Nationalsozialismus". Dieses Forschungsprojekt wird von der Stadt Kassel aufgrund eines Vertrages mit der Gesamthochschule gefördert. Grundlage dieser Förderung ist ein Beschluß aller Fraktionen der Kasseler Stadtverordnetenversammlung aus dem Jahre 1979, die Geschichte Kassels in der Zeit des Nationalsozialismus, insbesondere Verfolgung und Widerstand, zu untersuchen. Die Forschungsergebnisse werden der Stadt Kassel zur Verfügung gestellt. Unterlagen für dieses Forschungsvorhaben, wie Akten und Archivalien, sind in Kassel infolge Kriegszerstörung und Vernichtung von belastenden Dokumenten durch nationalsozialistische Stellen kaum vorhanden. Der Leiter des Forschungsprojekts hat zusammen mit dem Oberbürgermeister der Stadt Kassel die Staatskanzlei ersucht, ihm Zugang zu den Spruchkammerakten des ehemaligen Hessischen Ministeriums für Wiederaufbau und politische Befreiung zu gewähren. Darunter befinden sich auch die Akten für den NS-Gau Kurhessen und die frühere Gauhauptstadt Kassel. Forschungsziel ist die soziale Struktur der NSDAP-Mitgliedschaft im Raum Kassel. An einer namentlichen Kenntnis einzelner NSDAP-Mitglieder bestand von vornherein kein Interesse. Es ging vielmehr darum, aus den in den Akten enthaltenen Meldebogen sozialstrukturelle Daten über Alter, Geschlecht, Beruf, Bildung, Wohngebiet, Dauer der Parteizugehörigkeit, Parteifunktion u.ä. zu entnehmen und anonymisiert zu verwerten. Außerdem begehrten die Forscher Einblick in einige wenige Akten von Personen der Zeitgeschichte, z.B. regionalen NS-Führern wie Gauleitern . Diese Akteneinsicht sollte lediglich dazu dienen, andere bereits vorhandene Quellen wie Presseveröffentlichungen und die Dokumentation des Instituts für Zeitgeschichte auf ihre Zuverlässigkeit hin zu prüfen.

Der Hessische Ministerpräsident hat in einem Bescheid an den Oberbürgermeister dieses Ersuchen abgelehnt und auf § 3 Abs. 1 der Ersten Verordnung zur Durchführung des Dritten Gesetzes zum Abschluß der politischen Befreiung in Hessen vom 4. Dezember 1954 verwiesen. Auch eine zweite Eingabe des Oberbürgermeisters in dieser Angelegenheit wurde abgelehnt. Auf Bitten des Kulturpolitischen Ausschusses habe ich zu dieser Petition Stellung genommen mit dem Ergebnis, daß die Akteneinsicht durch die GHK nach der geltenden Rechtslage gestattet werden kann und die Ablehnung nicht in die Zuständigkeit des Hessischen Ministerpräsidenten fiel.

Ein letztes Beispiel: Eine wissenschaftssoziologische und historische Arbeit über die "Frankfurter Schule" der Sozialwissenschaften beschäftigt sich mit der Gründung des "Instituts für Sozialforschung" in den dreißiger Jahren. Quellen und Schriftwechsel dazu befinden sich im Archiv der Universität Frankfurt, die dem Forscher unter Hinweis auf den Daten- und Persönlichkeitsschutz den Zugang zu diesen Unterlagen verweigert. Schon in meinem Bericht über die Prüfung der Universität Frankfurt am Main (1980) habe ich auf das Fehlen von Rechtsvorschriften über Aufbewahrung und Benutzung von Archivgut der Universität hingewiesen. Über die Gestattung der Akteneinsicht wird nur im Einzelfall durch den Kanzler oder Präsidenten entschieden. Dabei waren in der Vergangenheit Kriterien wie z.B. die Reputation des Forschers, das Erkenntnisinteresse bzw. das Thema des Forschungsprojekts sowie auch informelle Mechanismen wie persönliche Kontakte für die Genehmigung mit entscheidend.

Die Institutionalisierung der Archive, die dauernde Aufbewahrung, Nutzung und Auswertung amtlicher Dokumente und Unterlagen, die schutzwürdigen Belange Betroffener, der postmortale Persönlichkeitsschutz und die Benutzung durch Dritte erfordern aus der Sicht eines Datenschutzes, der als Teil eines umfassenden Informationsrechts verstanden wird, eine Regelung in Form eines hessischen Archivgesetzes. Die Einfügung einer Archivklausel in das Hessische Datenschutzgesetz nach dem Vorbild anderer Landesdatenschutzgesetze (vgl. § 16 Abs. 3 Bremisches Datenschutzgesetz und § 13 Abs. 4 Rheinland-Pfälzisches Datenschutzgesetz) löst die Probleme nicht, da diese Klauseln keine ausreichende Rechtsgrundlage für eine Speicherung und Verwertung von personenbezogenen Daten durch Archive darstellen. Die Notwendigkeit einer Datenschutzregelung für Archive wird zusätzlich durch § 10 Abs. 5 S. 2 Melderechtsrahmengesetz und § 12 des Entwurfs des Hessischen Meldegesetzes unterstrichen; diese Bestimmungen sehen ausdrücklich Datenübermittlungen an das zuständige Archiv vor.

Die Landesregierung prüft gegenwärtig die Notwendigkeit eines Archivgesetzes. Zur Unterstützung der Diskussion möchte ich einen Entwurf für ein Hessisches Archivgesetz vorlegen, der in engem und ständigem Meinungsaustausch mit den hessischen Staatsarchiven entstanden ist.

Er hat folgende Fassung:

"Entwurf eines Gesetzes über die Sicherung und Nutzung von Archivgut für das Land Hessen
(Hessisches Archivgesetz)

§ 1

(1) Öffentliche Archive haben die Aufgabe, das Archivgut des Landes Hessen, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihrer Vereinigungen sowie ihrer Rechtsvorgänger auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten.

(2) Das Hessische Hauptstaatsarchiv und die Hessischen Staatsarchive bewahren das Archivgut des Landes und seiner Rechtsvorgänger auf. Die Zuständigkeit im einzelnen wird durch Rechtsverordnung geregelt.

§ 2

(1) Archivwürdig sind Unterlagen, die für die hessische und deutsche Geschichte unter Berücksichtigung ihrer politischen, ökonomischen, sozialen und kulturellen Bezüge von bleibendem Wert sind.

(2) Unterlagen können auf Dauer aufbewahrt werden, wenn sie für die Sicherung von Rechten des Bürgers und der Verfassungsorgane erheblich sind. Die Notwendigkeit der dauernden Aufbewahrung von Unterlagen zu Zwecken der Rechtswahrung in Archiven wird durch Rechtsvorschrift geregelt.

§ 3

(1) Archivgut sind alle archivwürdigen Unterlagen (Akten, Schriftstücke, Karteien, Dateien, Karten, Pläne, Bild-, Film- und Tonmaterialien) sowie sonstige Informationsträger, insbesondere maschinenlesbare Datenträger und die auf ihnen gespeicherten Informationen sowie Programme zu ihrer Auswertung, die bei den in § 1 genannten Stellen erwachsen oder in deren Besitz übergegangen sind.

(2) Zum Archivgut gehören auch archivwürdige Sammlungen von Dokumenten jeder Art, die von den in § 1 Abs. 1 genannten Stellen übernommen oder erworben worden sind, sonstige Bestände, die von den in § 1 genannten öffentlichen Archiven vor Inkrafttreten dieses Gesetzes erworben worden sind und Dokumentensammlungen, die von den Archiven zur Ergänzung des ihnen zukommenden Archivguts angelegt werden.

(3) Archivgut von Dienststellen, juristischen Personen oder Privaten, die nicht der Aufsicht des Landes unterliegen, kann auf vertraglicher Grundlage erworben oder in Verwahrung genommen werden, soweit an der Verwahrung und Erschließung öffentliches Interesse besteht. Dieses Archivgut unterliegt im Regelfall für die Dauer dieser Aufbewahrung den in diesem Gesetz für Aufbewahrung und Benutzung von Archivgut getroffenen Bestimmungen.

§ 4

(1) Die in § 1 genannten Behörden und sonstigen öffentlichen Stellen sind verpflichtet, alle Unterlagen, die zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind, zu sperren und auszusondern. Diese Unterlagen sind dem zuständigen Archiv zur Übernahme unverzüglich anzubieten.

(2) Akten, Dokumente und andere Informationsträger sind spätestens 30 Jahre nach ihrer Entstehung auszusondern, soweit nicht durch Rechtsvorschrift andere Fristen bestimmt werden. Akten, Dokumente und Informationsträger dürfen nur vernichtet werden, wenn das zuständige Archiv ein Interesse an der dauernden Aufbewahrung verneint hat. Dies gilt auch für die Löschung der nach § 19 Abs. 3 HDSG rechtmäßig gespeicherten Daten.

(3) Entscheidet das Archiv nicht binnen eines Jahres über die Archivwürdigkeit der angebotenen Unterlagen, dann sind sie zu löschen oder zu vernichten.

(4) Die Rechte des Betroffenen nach § 19 Abs. 3 S. 2 HDSG bleiben davon unberührt.

(5) Archivgut darf grundsätzlich nicht an andere Stellen als die zuständigen öffentlichen Archive abgegeben werden. In begründeten Ausnahmefällen ist im Benehmen mit dem zuständigen Archiv die Abgabe an ein anderes Archiv möglich, wenn die Einhaltung der in diesem Gesetz für die Aufbewahrung und Benutzung von Archivgut getroffenen Bestimmungen gewährleistet ist.

§ 5

(1) Das Archiv entscheidet im Benehmen mit der anbietenden Stelle über die Archivwürdigkeit der angebotenen Unterlagen und über die Übernahme in das Archiv.

(2) Fachkundigen Mitarbeitern des zuständigen Archivs ist Zutritt zu den Registraturen der in § 1 Abs. 1 genannten Stellen ihres Zuständigkeitsbereichs und Einsicht in die Findmittel und Dokumente dieser Registraturen zu gewähren.

(3) Das Archivgut ist zu erfassen, zu ordnen, zu verzeichnen, zu erhalten, instandzusetzen und für die Öffentlichkeit zugänglich zu machen.

(4) Hat der Träger eines Archivs keine Mitarbeiter, die über ausreichende Fachkunde verfügen, so ist die Wahrnehmung archivischer Aufgaben dadurch sicherzustellen, daß der Archivträger sich entweder der fachlichen Beratung durch ein öffentliches Archiv versichert oder das seiner Verfügung unterliegende Archivgut in einem öffentlichen Archiv hinterlegt.

§ 6

(1) Unterlagen, deren durch Rechtsnorm bestimmte Aufbewahrungsfrist noch nicht abgelaufen ist, können dem zuständigen Archiv als Zwischenarchivgut angeboten werden.

(2) Die Aufbewahrung und Nutzung von Zwischenarchivgut ist nur im Rahmen der Weisungen der abgebenden Stelle zulässig.

(3) Das Archiv hat für diese Unterlagen die technischen und organisatorischen Maßnahmen gem. § 6 HDSG zu treffen.

(4) Den durch Rechtsnorm bestimmten Aufbewahrungsfristen wird auch durch die Aufbewahrung im Archiv genügt. Archivwürdige Akten und Dokumente können vor Ablauf entsprechender Fristen in das zuständige Archiv übernommen werden.

§ 7

(1) Die dauernde Aufbewahrung und Benutzbarkeit des Archivguts sowie der Schutz vor unbefugter Nutzung oder Vernichtung sind durch technische und organisatorische Maßnahmen sicherzustellen.

(2) Soweit es sich um personenbezogene Unterlagen handelt, sind darüberhinaus technische und organisatorische Maßnahmen zur Datensicherheit i.S.v. § 6 HDSG und Anlage zu treffen. § 9 HDSG findet entsprechende Anwendung.

§ 8

(1) Jedermann hat das Recht, das in den öffentlichen Archiven verwahrte Archivgut nach Ablauf der festgelegten Sperrfristen zu amtlichen, wissenschaftlichen oder publizistischen Zwecken sowie zur Wahrung berechtigter persönlicher Belange zu benutzen, soweit durch dieses Gesetz oder aufgrund dieses Gesetzes nichts anderes bestimmt ist. Bestehende Informationsrechte oder besondere Vereinbarungen mit Eigentümern privaten Archivguts bleiben unberührt.

(2) Das Archivgut i.S.v. § 3 Abs. 1 ist für 30 Jahre seit der Entstehung der Unterlagen zu sperren, soweit nicht besondere Rechtsvorschriften dem entgegenstehen.

(3) Archivgut, das personenbezogene Daten enthält (personenbezogenes Archivgut), darf nicht vor Ablauf von 30 Jahren nach dem Tode des Betroffenen durch Dritte benutzt werden. Ist der Todestag nicht festzustellen, endet die Sperrfrist 100 Jahre nach der Geburt des Betroffenen. § 18 HDSG ist entsprechend anzuwenden. Amtsträger in Ausübung ihrer dienstlichen Obliegenheiten sind keine Betroffenen i.S.v. Satz 1.

(4) Die Sperrfristen nach Abs. 2 und 3 können im Einzelfall verkürzt oder höchstens um 20 Jahre verlängert werden, wenn dies im öffentlichen Interesse liegt. Bei personenbezogenem Archivgut ist die Verkürzung nur zulässig, wenn die Benutzung zu wissenschaftlichen Zwecken erfolgt und insbesondere durch Anonymisierung ausgeschlossen ist, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Die Genehmigung zur Benutzung von Archivgut ist einzuschränken oder zu versagen, wenn schutzwürdige Belange Dritter entgegenstehen oder der Erhaltungszustand des Archivguts gefährdet ist.

(6) Behörden darf Einsicht in personenbezogene Unterlagen nur für Zwecke gewährt werden, die nicht zu Maßnahmen gegen den Betroffenen oder seine Rechtsnachfolger führen. Diese Bestimmung gilt nicht für Unterlagen, die durch Rechtsverordnung für Zwecke der Rechtssicherung und Beweissicherung gem. § 2 Abs. 4 S. 2 zur dauernden Aufbewahrung bestimmt sind. Die Einsicht ist zu versagen, wenn die Unterlagen bei der abgebenden Stelle aufgrund besonderer Vorschriften zum Schutze des Betroffenen hätten gelöscht oder vernichtet werden müssen.

(7) Die Verknüpfung personenbezogener Informationen ist nur zulässig, wenn schutzwürdige Belange Betroffener nicht berührt werden.

(8) Die Benutzungsbedingungen werden im einzelnen durch eine besondere Benutzungsordnung geregelt.

§ 9

(1) Dem Betroffenen oder seinen Hinterbliebenen ist auf Antrag Auskunft über die im Archivgut zu seiner Person enthaltenen Daten zu erteilen.

(2) Das Archiv ist verpflichtet, eine Gegendarstellung des Betroffenen zu den Unterlagen, die sich auf seine Person beziehen, hinzuzufügen, wenn er durch falsche Tatsachenbehauptungen beeinträchtigt ist und ein berechtigtes Interesse an der Gegendarstellung glaubhaft macht.

(3) Die Gegendarstellung bedarf der Schriftform und muß von dem Betroffenen unterzeichnet sein. Sie muß sich auf Tatsachen beschränken und darf keinen strafbaren Inhalt haben.

(4) Diese Bestimmung gilt nicht für offizielle Berichte über öffentliche Sitzungen der gesetzgebenden oder beschließenden Körperschaften des Bundes, der Länder, der Gemeinden (Gemeindeverbände) und der Gerichte.

§ 10

(1) Öffentliche Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung können gemeinsame Forschungsarchive einrichten.

(2) Gemeinsame Archive haben die Aufgabe, die für bestimmte Forschungsvorhaben gespeicherten personenbezogenen Daten zu anonymisieren, zu aggregieren und für künftige Forschungszwecke bereitzuhalten. § 8 Abs. 7 gilt entsprechend. Die Übermittlung und Nutzung von Daten aus Forschungsarchiven ist nur für weitere Forschungszwecke zulässig.

(3) Die Merkmale, mit deren Hilfe anonymisierte Daten derart verändert werden können, daß sie sich auf eine bestimmte Person beziehen oder eine solche erkennen lassen, sind gesondert bei der Stelle zu speichern, die die Daten beim Betroffenen erhoben hat. Diese Daten sind zu löschen, wenn der Betroffene es verlangt oder wenn ihre Speicherung unzulässig war.

(4) Die Sperrfristen von § 8 finden auf anonymisierte Einzelangaben in Forschungsarchiven keine Anwendung, soweit durch die Art der Verwendung dieser Daten für weitere Forschungszwecke kein Grund zu der Annahme besteht, daß schutzwürdige Belange von Betroffenen beeinträchtigt werden.

§ 11

(1) Oberste Archivbehörde des Landes Hessen ist der Hessische Kultusminister.

(2) Der Kultusminister führt durch die ihm unterstellten Staatsarchive die Aufsicht über andere öffentliche Archive im Geltungsbereich dieses Gesetzes und regelt im Benehmen mit dem Landespersonalamt die Ausbildung und Prüfung der Archivare an öffentlichen Archiven durch Rechtsverordnung.

§ 12

Das Hessische Datenschutzgesetz vom 31. Januar 1978 (GVBl. S. 96) wird wie folgt geändert: An § 19 Abs. 3 S. 1 werden die Worte angefügt:
"und das zuständige Archiv ein Interesse an der Übernahme verneint hat."

§ 13

Das Gesetz tritt am ... in Kraft."

3.3
"Verrechtlichung" der Verarbeitung personenbezogener Daten durch die Polizei

Die Forderung nach einer "Verrechtlichung" - d.h. nach Rechtsvorschriften, die die Zulässigkeit der Verarbeitung personenbezogener Daten genau abgrenzen - für den Bereich der Sicherheitsbehörden zieht sich wie ein Leitmotiv durch die Tätigkeitsberichte des Hessischen Datenschutzbeauftragten. Bereits in dem - vor rund zehn Jahren vorgelegten - Ersten Tätigkeitsbericht (Drucks. 7/1495) heißt es: "Der Aufbau und die Unterhaltung eines solchen (Polizei-Informations-) Systems ist aus höherwertigen Interessen des Allgemeinwohls nur dann zu rechtfertigen, wenn Weitergabe und Verwendung der Informationen so eng wie möglich geregelt sind ..." (4.1.1.3.c). Der Zweite Tätigkeitsbericht für 1972 (Drucks. 7/3137) präzisiert diese Aussage: "Der Schutz des Persönlichkeitsrechts des Bürgers erfordert wegen der besonderen Empfindlichkeit der polizeilichen Daten eine **gesetzliche** Regelung (4.1.1.3.c).

Diese Forderung ist noch unter der Geltung des ersten Hessischen Datenschutzgesetzes vom 7. Oktober 1970 formuliert worden. An ihrer Aktualität hat sich seither nichts geändert. Das zweite Hessische Datenschutzgesetz vom 31. Januar 1978 hat zwar die Kontrollvoraussetzungen entscheidend verbessert. Der Prüfung des Datenschutzbeauftragten unterliegt jede Verarbeitung ohne Rücksicht darauf, ob sie maschinell oder manuell erfolgt. Auch alle herkömmlichen Akten werden, soweit sie durch automatisierte Verfahren erschließbar sind, in den Anwendungsbereich des HDSG einbezogen.
Eine wirksame Kontrolle der polizeilichen Informationsverarbeitung setzt aber klare Maßstäbe für deren Zulässigkeit voraus. An eindeutigen, gesetzlich abgesicherten Befugnisnormen fehlt es nach wie vor.

Zwar ist nicht zu verkennen, daß es im Bereich der Sicherheitsbehörden eine ganze Reihe von Richtlinien und Erlassen gibt, die einerseits die Aufgaben der einzelnen Behörden präzisieren und andererseits deren Informationsverhalten näher regeln. Gerade im letzten Jahr sind manche Verwaltungsvorschriften ergangen, die bezeichnend sind für den Versuch, dem Datenschutz Rechnung zu tragen. Die wohl besten Beispiele hierfür sind die KpS-Richtlinien ("Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen") vom 19. März 1981 (StAnz. S. 881) sowie die "Dateienrichtlinien" für das Bundeskriminalamt vom 26. Februar 1981.

Dennoch fehlt es für wichtige Bereiche polizeilichen Handelns selbst auf dieser untergesetzlichen Ebene noch an klaren Festlegungen. Diese Aussage bezieht sich z.B. auf die verbreitete Praxis des Fotografierens und Filmens von Bürgern zu allgemeinen "Dokumentationszwecken". Eine Reihe von Eingaben und Beschwerden erhärtet die Vermutung, daß der rechtliche Rahmen für Strafverfolgung und Gefahrenabwehr nicht immer eingehalten wird.

Insgesamt gilt jedoch nach wie vor, was im 8. Tätigkeitsbericht für 1980 (1.2.1) zu dem Entwurf der KpS-Richtlinien gesagt wurde: "... so wichtig Richtlinien gegenwärtig sind, sie dürfen . . . nicht als Instrument einer Dauerregelung gesehen und verstanden werden. Der Gesetzgeber muß vielmehr die mit ihrer Hilfe gewonnenen Erfahrungen nutzen, um sie so weit wie möglich durch gesetzliche Regelungen abzulösen. Die Richtlinien sind insofern . . . Zwischenstationen auf dem Weg zu gesetzlichen Vorschriften und deshalb ein Provisorium".

Diese Feststellung wird durch die bisherigen Erfahrungen in zweifacher Hinsicht unterstrichen:

1. Im Laufe von Prüfungen hat sich gezeigt, daß notwendige, in den Richtlinien vorgesehene Datenschutzvorkehrungen, beispielsweise die Durchführung der Bestimmungen über die Löschung, immer wieder hinausgeschoben werden. Offensichtlich erzeugen Verwaltungsvorschriften einen weitaus geringeren Anwendungsdruck als gesetzliche Bestimmungen.

2. Auch die Vielzahl vorhandener Richtlinien konnte nicht verhindern, daß einzelne Sicherheitsbehörden ihre Befugnis, personenbezogene Daten zu verarbeiten, sehr weit interpretieren. Die gesetzlich vorgesehene Trennung sowohl der Aufgabenbereiche von Gefahrenabwehr und Strafverfolgung - bezogen auf den Inhalt der Tätigkeit - als auch der Polizei und des Verfassungsschutzes - bezogen auf die Institutionen - wird durch die bestehenden Verwaltungsvorschriften nicht ausreichend verdeutlicht. Ein besonders bezeichnendes Beispiel dafür ist die präventive Tätigkeit der polizeilichen Staatsschutzabteilungen. Organisatorisch der Kriminalpolizei zugeordnet, sammeln diese Behörden auch Daten im Vorfeld von Straftaten. Je weiter und umfassender ihre Aktivität in dieses Vorfeld auch nur möglicherweise in Betracht kommender strafbarer Handlungen ausgedehnt wird, desto deutlicher zeichnet sich die Gefahr ab, nicht nur über die Vermengung von Strafverfolgung und Gefahrenabwehr den eigenen Zuständigkeitsbereich zu überschreiten, sondern zugleich unzulässigerweise Aufgaben des Verfassungsschutzes zu übernehmen. Zudem: Polizeiliche Gefahrenabwehr setzt stets das Vorliegen einer "konkreten Gefahr" voraus. Die Beobachtung verfassungsfeindlicher Bestrebungen ist, soweit diese Voraussetzung nicht gegeben ist, nicht Aufgabe der Polizei. Die gerade im Hinblick auf diese Entwicklung begonnenen Prüfungen werden im kommenden Jahr verstärkt fortgesetzt werden.

Die Forderung nach einer gesetzlichen Regelung kann auch nicht durch einen Hinweis auf das HDSG entkräftet werden. Das HDSG enthält zwar in den §§ 11, 12 und 16 allgemeine Befugnisnormen für die Speicherung und Übermittlung personenbezogener Daten durch öffentliche Stellen. Diese beziehen sich aber - ihrem Charakter als Auffangbestimmungen entsprechend - nur generell auf die Erforderlichkeit zur Aufgabenerfüllung. Sie können also für sich genommen nicht hinreichend klar abgrenzen, ob eine Datenverarbeitung durch die Polizei im Einzelfall zulässig ist oder nicht.

Aus dem gleichen Grund hatte ich im 9. Tätigkeitsbericht (2.4.) eine besondere gesetzliche Regelung für den Verfassungsschutz gefordert. Ähnlich wie dort müssen auch für die Polizei Befugnisnormen konkret festlegen, "unter welchen Voraussetzungen Daten erhoben, gespeichert und verändert werden dürfen, wem und zu welchem Zweck die Polizeibehörden diese Daten übermitteln dürfen, von wem ihnen Daten übermittelt werden und wann diese Daten zu berichtigen bzw. zu löschen sind". Diese Normierungsaufgabe wird nicht zuletzt dadurch erleichtert, daß die KpS-Richtlinien eine Reihe durchaus übernehmbarer Regelungsansätze enthalten (vgl. dazu 2.2.2).

3.4
Krebsregister-Gesetz

Die Diskussion über die Einrichtung von Krebsregistern (vgl. zum aktuellen Stand in Hessen oben 2.3.3) ist seit dem letzten Tätigkeitsbericht in ein neues Stadium getreten. Es ist durch folgende Aspekte gekennzeichnet:

- Unter dem Einfluß der Auseinandersetzung über die Datenschutzprobleme bei medizinischer Forschung hat manche, in der Vergangenheit nicht ausreichend zur Kenntnis genommene Vorschrift des ärztlichen Berufsrechts und des Strafrechts an Bedeutung gewonnen. Gemeint sind insbesondere die Bestimmungen über die ärztliche Schweigepflicht und über die Wahrung des Berufsgeheimnisses. Sie und nicht die Vorschriften der Datenschutzgesetze sind es, die in erster Linie den Konflikt zwischen der Krebsforschung und dem Interesse der Patienten an der Geheimhaltung ihrer Gesundheitsdaten verursachen.

- Der Bedarf an personenbezogenen Patientendaten für die medizinische Forschung wird von großen Berufsverbänden der Ärzte offenbar keineswegs so dringlich eingeschätzt, daß sie dafür die standesrechtlichen Regelungen über die ärztliche Schweigepflicht abzuändern bereit wären. Zudem ist es den Epidemiologen nach wie vor nicht gelungen, klarzustellen, warum die Forderung, für die Meldung an das Krebsregister die Einwilligung des Patienten einzuholen, die Aussagefähigkeit des Registers beeinträchtigt. Immerhin haben von der Bundesregierung bestellte Gutachter noch 1980 "für den angestrebten Zweck eine repräsentative Stichprobe von 10 bis 15 v.H. der Gesamtbevölkerung in einer der Struktur der Bundesrepublik Deutschland möglichst gut entsprechenden Gebietsauswahl" als "ausreichend" angesehen (BT-Drucks. 8/3556, Anl. 1, S. 34).

  Da in dem von der "Großen Krebskonferenz" vorgelegten Modellentwurf für ein Krebsregister-Gesetz (vgl. oben 2.3.3) eine Pflicht der Ärzte zur Meldung aller Fälle nicht vorgesehen ist, kann aufgrund der Freiwilligkeit der Meldung eine vollständige Registrierung aller Krebskranken ohnehin nicht erreicht werden. Wer deshalb die Forderung nach der Einwilligung der Betroffenen für unvertretbar hält, müßte darlegen, inwiefern eine Lösung ohne Information des Patienten zu repräsentativen Ergebnissen führen kann.

- Das Krebsregister ist zum Anlaß genommen worden, die Registrierung weiterer Krankheiten zu Zwecken der medizinischen Forschung anzustreben. Rechtlich sollen solche Bestrebungen, sei es mit Hilfe eines allgemeinen Epidemiologieregister-Gesetzes, sei es durch Einfügung einer entsprechenden "Registerklausel" in die Landesdatenschutzgesetze, abgesichert werden.

In Anbetracht dieser Entwicklung haben die Datenschutzbeauftragten der Länder und des Bundes in ihrer Sitzung vom 14. Dezember 1981 folgende Erklärung verabschiedet:

1. Die Datenschutzbeauftragten erkennen die gesundheitspolitische Bedeutung der medizinischen Forschung, insbesondere im Zusammenhang mit der Bekämpfung von Krebserkrankungen, an. Es entspricht ihrer gesetzlichen Aufgabe, auch in diesem Bereich für die Wahrung der schutzwürdigen Belange der Patienten einzutreten. Ihre Bedenken und Vorschläge zielen daher ausschließlich darauf ab, die Freiheit der Forschung in ein ausgewogenes und rechtlich abgesichertes Verhältnis zu den grundrechtlich geschützten Belangen der Betroffenen zu bringen. Sie gehen davon aus, daß es möglich ist, Regelungen zu finden, die den Erfordernissen der Forschung wie auch des Schutzes der Individualsphäre gerecht werden. Die gelegentlich geäußerte pauschale Behauptung, der Datenschutz behindere die Krebsforschung, weisen sie als unbegründet zurück.

2. Es ist nicht die Aufgabe der Datenschutzbeauftragten, Sinn und Nutzen von Krebsregistern zu beurteilen. Sie warnen aber nachdrücklich vor der Gefahr, daß die Gesetzgebung zum Krebsregister ein erster Schritt zur Errichtung einer Vielzahl anderer Epidemiologieregister werden könnte. In diesem Zusammenhang weisen sie darauf hin, daß auch aus Kreisen der Ärzteschaft erhebliche Zweifel am Nutzen medizinischer Register geäußert werden, woraus sich Zweifel an der Erforderlichkeit derartiger Register ableiten lassen. Sie appellieren an die medizinische Forschung, stärker als bisher den bereits vorhandenen Forschungsstand zur Anonymisierung personenbezogener Daten zu nutzen und sich vordringlich um die Weiterentwicklung von Anonymisierungs- und Aggregationsmethoden zu bemühen. Diese methodologischen Überlegungen können wesentlich dazu beitragen, Probleme, die sich durch die ärztliche Schweigepflicht und den Datenschutz ergeben, gar nicht erst aufkommen zu lassen.

3. Für den Fall der politischen Entscheidung in den Ländern zugunsten der Schaffung von Krebsregistern halten die Datenschutzbeauftragten es für notwendig, daß die Errichtung, Ausgestaltung und Nutzung von Krebsregistern in einem speziellen Gesetz geregelt werden. Wesentliche Eingriffe in Grundrechtspositionen der Betroffenen sind nur durch ein Gesetz zu legitimieren, das die nachfolgenden Grundsätze beachtet (vgl. unten 4.). Dabei wird davon ausgegangen, daß es sich um ein Register zur Erfassung der Anzahl der Neuerkrankungen (Inzidenzregister) bzw. der Anzahl erkrankter Personen (Prävalenzregister) handeln wird. Eine im Anwendungsbereich unbestimmte allgemeine Rahmenregelung für die medizinische Forschung in einem Landesdatenschutzgesetz, die derzeit im Vordergrund baden-württembergischer Überlegungen steht, lehnen die Datenschutzbeauftragten daher - auch aufgrund verfassungsrechtlicher Bedenken - ab.

4. Nach Auffassung der Datenschutzbeauftragten muß ein Krebsregistergesetz zumindest die folgenden Prinzipien berücksichtigen:

(1) Die Meldung von Patientendaten mit Personenbezug an das Krebsregister bedarf grundsätzlich der Einwilligung des Betroffenen (bzw. der Entbindung von der ärztlichen Schweigepflicht). Nur ausnahmsweise kann die Meldung auch ohne Einwilligung des Patienten erfolgen, und zwar wenn sie für die Zwecke des Krebsregisters nachweisbar notwendig ist und dem Patienten dadurch, daß ihm die Art seiner Erkrankung bekannt wird, gesundheitliche Nachteile entstehen können. Soweit weder ein solcher Ausnahmefall noch eine Einwilligung vorliegt, unterbleiben Meldungen an das Register. Der zulässige Umfang der Einwilligung ist im Gesetz festzulegen.

(2) Für die weitere Übermittlung durch das Krebsregister an andere Forschungseinrichtungen ist grundsätzlich eine besondere Einwilligung erforderlich, wenn die Daten nicht in aggregierter oder anonymisierter Form weitergegeben werden. Für diese Übermittlung ist entsprechend der Regelung über die Forschung mit Sozialdaten ein Genehmigungsverfahren vorzusehen. Eine nochmalige Übermittlung durch die Forschungseinrichtung an Dritte ist unzulässig.

(3) Der Gesetzeszweck, die Aufgaben des Krebsregisters, seine Rechtsform und institutionelle Ausgestaltung sind im Gesetz festzulegen. Im Interesse einer wirksamen Aufsicht sollte das Krebsregister in öffentlich-rechtlicher Trägerschaft geführt werden.

(4) Der Kreis derjenigen Institutionen, die zu Forschungszwecken personenbezogene Daten des Krebsregisters erhalten können, sollte in der Weise beschränkt werden, daß die ausschließliche Verwendung zu Forschungszwecken gewährleistet ist. Dies bedingt eine externe Kontrolle des Datenschutzes von Amtswegen.

(5) Der in den Statistikgesetzen verankerte Grundsatz der Zweckbindung muß auch für die im Krebsregister gespeicherten Daten gelten. Im übrigen sollte geprüft werden, ob ein gesetzliches Verbot eingeführt werden sollte, vom Betroffenen eine Bescheinigung über den Inhalt der im Krebsregister gespeicherten Daten zu verlangen. Ein solches Verbot könnte verhindern, daß potentielle Arbeitgeber oder sonstige Vertragspartner vom Betroffenen die Vorlage einer Art Negativattest des Krebsregisters fordern.

(6) Eine Verknüpfung mit anderen Datenbanken ist unzulässig.

(7) Die Aufbewahrung personenbezogener Daten beim Krebsregister ist zu befristen. Patientendaten sind außerdem zu löschen, wenn sie nicht mehr benötigt werden.

(8) Jeder Betroffene hat Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten aus dem Krebsregister. Dies gilt auch für Patienten, die über die Meldung nicht informiert worden sind. Entsprechend den Regelungen für Sozialdaten in § 25 SGB X kann bei Gefahr für die Gesundheit des Patienten die Auskunft vermittelt durch einen Arzt erteilt werden.

4. Datenschutzprobleme - Erfahrungen und Beispiele

4.1
Datenschutz im Sozialbereich

4.1.1
Tätigkeitsschwerpunkte 1981

4.1.1.1
Überblick

Am 1. Januar 1981 ist das Zehnte Buch des Sozialgesetzbuchs (SGB X) in Kraft getreten. In seinem Zweiten Kapitel (§§ 67 ff.) enthält es eine ausführliche Regelung über die Wahrung des Sozialgeheimnisses und den Schutz der Sozialdaten. Über Anlaß und Inhalt dieser Novellierung gibt bereits mein letzter Tätigkeitsbericht eine kurze Information (vgl. 9. Tätigkeitsbericht, 3.3). Dort hatte ich als Hauptaufgabe für dieses Berichtsjahr definiert, "den Inhalt der neuen Vorschriften in den betroffenen Behörden intensiv bekannt zu machen", und diese Feststellung mit meinem Angebot der Beteiligung an einschlägigen Informationsveranstaltungen verknüpft. Von diesem Angebot haben die Behörden bzw. Mitarbeiter der hessischen Sozialverwaltung regen Gebrauch gemacht.

Was den Datenschutz im Sozialbereich angeht, lassen sich die Schwerpunkte meiner Tätigkeit im Jahre 1981 wie folgt zusammenfassen:

1. die Vermittlung von Informationen über das SGB X an Landesbehörden, Sozialversicherungsträger, Kommunen, aber auch an Verbände der freien Wohlfahrtspflege;

2. die Klärung von bzw. die Stellungnahme zu strittigen oder unklaren Einzelfragen der Interpretation, die bei einem neuen Gesetz ohne vorhergehende Kodifikation besonders häufig sind und

3. die Hilfestellung für die Praxis bei der Realisierung der aufgrund des SGB X zu ziehenden Konsequenzen für die Änderung von Verwaltungsabläufen.

Diese Schwerpunktsetzung ergab sich nicht nur deshalb, weil es sich beim SGB X um das erste umfassende bereichsspezifische Gesetzgebungswerk nach dem Inkrafttreten der Datenschutzgesetze von Bund und Ländern im Jahre 1978 handelt. Sie verdeutlicht vielmehr auch, daß für den Datenschutzbeauftragten die Verhinderung von Datenschutzverstößen, d.h. die Information und Beratung der Verwaltung vor Entscheidungen und Maßnahmen mit Datenschutzbezug, Vorrang hat vor der Korrektur von Mißständen und der Beanstandung fehlerhafter Gesetzesanwendung im nachhinein. Beispielhaft aufzeigen läßt sich weiterhin, wie meine Aufgaben und Befugnisse der Beratung, der Präsentation von konkreten Vorschlägen an die betroffenen Behörden und der Kontrolle "vor Ort" auf den unterschiedlichen Verwaltungsebenen ineinandergreifen, um eine optimale Verwirklichung des Datenschutzes zu gewährleisten.

4.1.1.2
Beratung der Aufsichtsbehörden und Spitzenverbände

Die Beratungstätigkeit gegenüber den Aufsichtsbehörden der Sozialverwaltung, den Verbänden der Leistungsträger und den kommunalen Spitzenverbänden hatte zum Ziel, diese in die Lage zu versetzen, ihre eigenen Aufgaben der Überwachung, Koordination oder Beratung im Bereich des Sozialdatenschutzes effektiver erfüllen zu können. Daraus ergibt sich eine wichtige "Multiplikatorwirkung" bei der Umsetzung der gesetzlichen Vorgaben. Im Sinne dieser Zielsetzung habe ich z.B. gegenüber dem Hessischen Sozialminister und dem Hessischen Städtetag zu einer Reihe von Einzelfragen des SGB X Stellung genommen (Beispiele dazu unten 4.1.3.2, 4.1.3.3 und 4.5.8).

4.1.1.3
Mitarbeiterschulung

Der Zusammenarbeit auf der Ebene der Aufsichtsbehörden und Verbände steht an Bedeutung nicht nach die direkte Information der Verwaltungspraktiker "vor Ort", der Referenten, Amtsleiter und Sachbearbeiter, die das neue Gesetz beachten bzw. anwenden müssen. Für diesen Personenkreis haben meine Mitarbeiter auf einer Vielzahl von Schulungs- und Fortbildungsveranstaltungen referiert, die u.a. vom Landespersonalamt, vom Hessischen Städtetag, vom Deutschen Verein für öffentliche und private Fürsorge sowie von einzelnen Kommunen für ihre Beschäftigten in den Sozial- und Jugendämtern abgehalten worden sind.

4.1.1.4
Kontrollen und Prüfbesuche

Bei Gelegenheit von Prüfbesuchen bei einzelnen Sozialleistungsträgern habe ich kontrolliert, inwieweit die Bestimmungen des SGB X organisatorisch - etwa durch entsprechende Verfügungen - und technisch, d.h. im Bereich der automatisierten Datenverarbeitung, umgesetzt worden sind. Natürlich können derartige Informations- und Kontrollbesuche nach § 23 Abs. 1 HDSG nur stichprobenweise durchgeführt werden. Im Jahre 1981 wurde dafür eine große gesetzliche Krankenkasse (AOK Wiesbaden) und eine Kommunalverwaltung mit einer Reihe von Ämtern, die Sozialleistungen abwickeln, ausgewählt (Kreisverwaltung Waldeck-Frankenberg). Die nach diesen Prüfungen erstellten umfangreichen Berichte sollen nicht nur der jeweils aufgesuchten Stelle helfen, Schwachstellen von Datenschutz und Datensicherung zu erkennen und Mängel abzustellen. Sie sind vielmehr auch Grundlage für Anregungen und Vorschläge zur Verbesserung des Datenschutzes gegenüber anderen vergleichbaren Behörden, gegenüber dem Hessischen Sozialminister oder den Dach- und Spitzenverbänden der Sozialleistungsträger. Ergebnisse aus diesen beiden Berichten sind auszugsweise wiedergegeben unten 4.4.3.6 und 4.4.3.7).

4.1.2
Leitlinien für die Auslegung - die Grundprinzipien des 2. Kap. SGB X

Die große Zahl der Anfragen zu Auslegungs- und Anwendungsproblemen der Regelungen über den Sozialdatenschutz beweist, wie ernst die Wahrung des Sozialgeheimnisses von den Leistungsträgern bzw. ihren Mitarbeitern genommen wird. Sie verrät allerdings auch, daß im Gestrüpp der Einzelfragen der täglichen Verwaltungspraxis die grundlegenden Prinzipien und Ziele des SGB X aus dem Blickfeld zu geraten drohen. Diese wesentlichen Grundsätze lauten:

1. Die Weitergabe von Sozialdaten ist abschließend geregelt. Ihre Zulässigkeit setzt voraus, daß entweder die Einwilligung des Betroffenen oder eine gesetzliche "Offenbarungsbefugnis" nach §§ 67 bis 78 SGB X vorliegt.

2. Der für die Aufgaben der Sozialverwaltung erforderliche Datenfluß bleibt von der Neuregelung unberührt. Von den gesetzlich genannten Ausnahmefällen abgesehen, stehen Sozialdaten jedoch für andere Verwaltungszwecke oder private Interessen nicht zur Verfügung.

3. Alle Daten, auch die "Personalien" wie Name, Anschrift, Geburtstag usw. sind geschützt; besonderem Schutz unterliegen "sensitive", d.h. z.B. medizinische und psychologische Angaben.

4. Für die Empfänger von Sozialdaten (öffentliche Stellen oder Privatpersonen) gilt der Grundsatz der Zweckbindung und ebenfalls die Pflicht zur Wahrung des Sozialgeheimnisses.

5. Für alle Sozialleistungsträger - ob auf Bundes-, Landes- oder kommunaler Ebene - gilt einheitliches Datenschutzrecht, d.h. neben dem SGB X ergänzend das Bundesdatenschutzgesetz.

6. Für die Übermittlung von Sozialdaten im Wege der Amtshilfe an die Behörden außerhalb der Sozialverwaltung gilt das Prinzip der "Entscheidungsverlagerung nach oben". Entscheidungsbefugt ist nicht der einzelne Sachbearbeiter, sondern - im einzelnen unterschiedlich - der Behördenleiter, sein Stellvertreter oder ein besonders bevollmächtigter Bediensteter.

7. Bei der Übermittlung für Forschungs- und Planungsvorhaben im Sozialleistungsbereich ist ein Genehmigungsverfahren einzuhalten.

8. Soweit eine Offenbarung nicht zulässig ist, besteht keine Auskunftspflicht, keine Zeugnispflicht (etwa vor Gericht) und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, Akten, Dateien und sonstigen Datenträgern.

4.1.3
Konsequenzen aus dem SGB X

4.1.3.1
Weitergabe von Sozialdaten: Notwendige Änderungen in der Verwaltungspraxis

Sozialleistungsträger verfügen über Daten, die häufig aktueller und vollständiger sind als die Angaben über die gleiche Person in anderen Verwaltungsbereichen. Wer etwa Leistungen bei der Krankenkasse beantragt, wird schon deshalb seine richtigen Personalien angeben, um die Leistung auch zu erhalten; bei der Meldebehörde dagegen hat der gleiche Bürger sich möglicherweise nicht an-, ab- oder umgemeldet. Der Außendienst des Sozial-oder des Jugendamts holt eine ganze Reihe von Informationen über die Privatsphäre von Klienten ein, die auch für polizeiliche Ermittlungen von großem Interesse sein können. Die beiden Beispiele sollen illustrieren, wie vielfältig die Interessen anderer Behörden und Stellen sein können, an den Datenbeständen der Sozialverwaltung zu partizipieren und sie für ihre Zwecke zu nutzen.

Das SGB X erteilt jedoch Vorstellungen von einer uneingeschränkten "Amtshilfe" mit Sozialdaten eine klare Absage. Die persönlichen Angaben der Sozialhilfeempfänger, der Rentenversicherten oder der Arbeitslosen - kurz: die "Sozialdaten" - sollen grundsätzlich nur für die Aufgabenerfüllung der Sozialbehörden zur Verfügung stehen. Unter welchen Bedingungen und in welchem Umfang Datenanforderungen z. B. der Finanzämter, der Polizei oder der Gerichte eine Ausnahme von diesem Grundprinzip rechtfertigen, hat der Gesetzgeber selbst und abschließend entschieden. Um den einzelnen Sachbearbeiter mit der häufig nicht einfachen Entscheidung über die Anwendbarkeit einer Offenbarungsvorschrift nicht zu belasten oder zu überfordern, weist das SGB X diese Entscheidung in einer Reihe von Fällen dem Vorgesetzten (Amts- bzw.Behördenleiter), dem Richter oder der Aufsichtsbehörde zu.

Dies bedeutet, daß manche in der Verwaltungspraxis der Sozialbehörden üblichen und eingespielten Kommunikationswege und Entscheidungsstränge geändert werden müssen. Mein Bericht über die Prüfung der Landkreisverwaltung Waldeck-Frankenberg enthält zur behördeninternen Umsetzung dieser Konsequenz den Vorschlag, eine Geschäftsanweisung über die Weitergabe von Sozialdaten im Wege der Amtshilfe zu erlassen. Sie sollte mindestens die folgenden Punkte beinhalten:

1. Über Ersuchen anderer Stellen um Übermittlung von "Personalien" (außerhalb der speziell geregelten Fälle unten 2. bis 5.), d.h. von Name, Anschrift, Geburtsdatum usw. der Klienten des Sozial- und Jugendamtes sowie aller anderen Ämter, die Sozialdaten verarbeiten, darf nicht der einzelne Sachbearbeiter entscheiden; vielmehr ist der jeweilige Leiter der ersuchten Stelle, sein Stellvertreter oder ein dazu besonders bevollmächtigter Bediensteter dafür zuständig (§ 68).

2. Informationswünschen von Staatsanwaltschaft und Kriminalpolizei zur Aufklärung von Straftaten darf nur nachgekommen werden, wenn eine richterliche Anordnung vorliegt, es sei denn, es handelt sich um

- Straftaten, die mit der Abwicklung von Sozialleistungen zusammenhängen (z.B.: Betrug bei Sozialhilfe)
- lediglich die "Personalien", s.o. 1. (§ 73).

3. Ersuchen um Weitergabe von Sozialdaten seitens der Verfassungsschutzämter, anderer Nachrichtendienste (MAD, BND) und des Bundeskriminalamtes dürfen nur vom Landrat selbst oder seinem allgemeinen Vertreter entschieden werden (§ 72).

4. Auskunftsersuchen von Personen, die einen gesetzlichen oder vertraglichen Unterhaltsanspruch oder einen Anspruch im Rahmen des Versorgungsausgleichs geltend machen, dürfen erst beantwortet werden, nachdem der auskunftspflichtige Anspruchsgegner von dem zuständigen Amt gemahnt worden und seiner Auskunftspflicht in angemessener Zeit nicht nachgekommen ist (§ 74).

5. Die Offenbarung zu Zwecken der Forschung und Planung (z.B. Akteneinsicht durch Hochschullehrer oder Diplomanden zu Forschungszwecken) bedarf der vorherigen Genehmigung durch die zuständige oberste Landesbehörde (hier: durch den Hessischen Sozialminister) (§ 75).

6. Die Zweckbindung und Geheimhaltung bei den Empfängern von Sozialdaten ist durch geeignete Vorkehrungen (z.B. schriftlicher Hinweis auf die Einhaltung des Sozialgeheimnisses) zu gewährleisten (§ 78).

7. Die Weitergabe von Sozialdaten zu Zwecken der gesetzlichen Aufgabenerfüllung - etwa nach dem JWG, BSHG usw. -, also der Regelfall in der täglichen Praxis, ist nach wie vor zulässig (§ 69 Abs. 1 Nr. 1). Als Einschränkung ist jedoch der Grundsatz der "Erforderlichkeit" zu beachten: So dürfen beispielsweise komplette Akten dann nicht übersandt werden, wenn lediglich ein Bericht oder eine Auskunft zu einzelnen Fragen angefordert wurde.

8. Mit der schriftlichen Einwilligung des Betroffenen im Einzelfall ist die Übermittlung seiner Daten immer zulässig (§ 67).

Zwar ist der vorstehende Text in einzelnen Punkten speziell auf die Gegebenheiten der Kommunalverwaltung zugemünzt. Die dringende Anregung, die Handhabung der Übermittlung von Sozialdaten durch entsprechende Richtlinien, Anweisungen, Verfügungen o.ä. an die betroffenen Mitarbeiter so zu regeln, daß die §§ 67 ff. SGB X eingehalten werden, richtet sich jedoch an alle Sozialleistungsträger in Hessen, die bisher noch keine Vorkehrungen getroffen haben.

4.1.3.2
"Behördenbegriff" und Geltung des SGB X innerhalb von Stadt- und Kreisverwaltungen

Die Arbeitsgruppe "Datenschutz" der Bundesvereinigung der kommunalen Spitzenverbände hat sich dafür ausgesprochen, "auch für die Anwendung des Sozialgesetzbuches den organisationsrechtlichen (ganzheitlichen) Behördenbegriff zugrunde zu legen". Der Sozialausschuß des Hessischen Städtetages hat sich dieser Auffassung angeschlossen. Gemeint ist damit, daß die präzisen, engen Regelungen über die Offenbarung von Sozialdaten (§§ 35 SGB I, 67 ff. SGB X) gegenüber anderen Ämtern der gleichen kommunalen Gebietskörperschaft keine Anwendung finden sollen, sondern nur bei der Übermittlung an Stellen außerhalb der Kommunalverwaltung - für die Reichweite und Schutzwirkung des Sozialgeheimnisses in den Kommunen eine äußerst wichtige Frage (grundsätzlich zum "funktionalen Stellenbegriff" unten 4.3).

Diese Auffassung ist aus folgenden Gründen unrichtig:

- Gerade die in der kommunalen Sozialverwaltung (z.B. im Jugendamt, in städtischen Erziehungs- oder Drogenberatungsstellen) verarbeiteten personenbezogenen Daten sind besonders "sensitiv" und damit besonders schutzbedürftig. Die Wahrung des Sozialgeheimnisses hat dort aber nicht nur im Interesse des Schutzes der Privatsphäre der Klienten, sondern auch im Hinblick auf die Funktionsfähigkeit der Sozialarbeit selbst ("Vertrauensverhältnis zum Hilfesuchenden") besonderes Gewicht.

- Eine Weitergabe von Sozialdaten ohne Beachtung des SGB X innerhalb der Kommunalverwaltung würde dazu führen, daß Sozialdaten für eine Vielzahl von Verwaltungszwecken - etwa des Ausländeramts, des Ordnungsamts, der Führerscheinstelle usw. - ohne quantitative Beschränkung zur Verfügung stehen. Dies widerspricht jedoch dem bereits mehrfach angeführten Grundprinzip des SGB X, daß die Datenbestände der Sozialbehörden außer in den gesetzlich ausdrücklich normierten Ausnahmefällen nur zur Erfüllung sozialer Aufgaben verwandt werden sollen.

- Die Auffassung der Spitzenverbände findet auch aus einem anderen Grund im Gesetz keine Stütze. Sicherlich sind die kreisfreie Stadt bzw. der Kreis als solche insofern als "Sozialleistungsträger" anzusehen, als die Verantwortlichkeit für Durchführung und Finanzierung gemeint ist. Adressaten der Übermittlungsnormen der §§ 67 ff. ("Sozialgeheimnis-Träger") können jedoch nur diejenigen Stellen oder Ämter sein, die Sozialdaten verarbeiten. Außerdem ergibt sich aus den Mitteilungsbefugnissen in § 71 Nr. 2 SGB X, daß die Übermittlung an das Gesundheits- und das Ausländeramt, also an Ämter innerhalb der übergreifenden Verwaltungseinheiten Stadt oder Kreis, vom Gesetzgeber als Einzelfälle zulässiger Offenbarung für regelungsbedürftig gehalten wurden.

Diese Argumente zeigen, daß die Offenbarungsbestimmungen des SGB X auch für den Datenaustausch zwischen kommunalen Ämtern mit Sozialleistungsaufgaben und Ämtern mit anderen Verwaltungsaufgaben Anwendung finden. Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat diese übereinstimmende Auffassung in einem entsprechenden Beschluß vom 14. Dezember 1981 bekräftigt. Bei Anfragen und Kontrollen werde ich auch in Zukunft von dieser Interpretation ausgehen. Die hessischen kommunalen Spitzenverbände, den Hessischen Sozialminister und den Hessischen Innenminister (als oberste Kommunalaufsichtsbehörde) habe ich über meine Ansicht unterrichtet.

4.1.3.3
"Datenschutzbeauftragte" für die kommunale Sozialverwaltung

Das SGB X bringt für die Kontrolle des Datenschutzes im öffentlichen Bereich eine wichtige Neuerung. § 79 Abs. 1 SGB X statuiert erstmals auch für einen Teil der Behörden und Körperschaften des öffentlichen Rechts - eben die öffentlich-rechtlichen Sozialleistungsträger - die gesetzliche Verpflichtung, einen Datenschutzbeauftragten zu bestellen. Einen internen Datenschutzbeauftragten kennen die Datenschutzgesetze ansonsten nur für den nichtöffentlichen Bereich (§§ 28, 29 BDSG). Allerdings hat der Hessische Minister des Innern mit Erlaß vom 2. Oktober 1978 (StAnz. S. 2011) die Behörden des Landes Hessen aufgefordert, einen Bediensteten mit der Aufgabe der Überwachung des Datenschutzes zu betrauen; den Gemeinden wurde empfohlen, ebenso zu verfahren.

Auch in dieser Frage herrscht eine erhebliche Rechtsunsicherheit: In mehreren Stellungnahmen von Gremien kommunaler Spitzenverbände auf Bundes- und hessischer Ebene wird die Verpflichtung aus § 79 SGB X als für die Kommunen nicht geltend bezeichnet und ihnen empfohlen, keinen "Datenschutzbeauftragten" nach dieser Bestimmung zu bestellen. Als Begründung werden in erster Linie verfassunsrechtliche Argumente angeführt; die Vorschrift des § 79 Abs. 1 SGB X stelle insoweit einen unzulässigen Eingriff in die kommunale Organisationshoheit dar. Entgegen dieser Auffassung hat sich u. a. der Bayerische Staatsminister des Innern dahingehend geäußert, daß auch die Kommunen für den Bereich ihrer Sozialbehörden einen Datenschutzbeauftragten benennen müssen.

Dazu ist folgendes festzuhalten:

1. Aus § 79 Abs. 1, 2. Halbsatz SGB X i.V.m. der entsprechenden Anwendung der §§ 28, 29 BDSG ergibt sich eine gesetzliche Verpflichtung auch für die Städte und Kreise, einen Bediensteten zum Verantwortlichen für die Sicherstellung der Ausführung der Bestimmungen über den Schutz der Sozialdaten zu bestellen, wenn das Mindestquorum bei der Datenverarbeitung Beschäftigter erfüllt ist. Auf die Bezeichnung "Datenschutzbeauftragter" kommt es dabei nicht an.

2. Anforderungsprofil Stellung und Aufgabenbereich dieses Mitarbeiters ergeben sich grundsätzlich aus §§ 28, 29 BDSG. Abweichungen - wegen der lediglich "entsprechenden" Anwendbarkeit dieser Normen auf Sozialleistungsträger - sind nur da zulässig, wo Besonderheiten der kommunalen Verwaltungsstruktur dies zwingend erfordern. Dieser Bedienstete muß daher

   - die erforderliche Sachkunde und Zuverlässigkeit besitzen
   - auf dem Gebiet des Sozialdatenschutzes weisungsfrei sein
   - der Behördenleitung für die Aufgabe des Sozialdatenschutzes unmittelbar unterstellt sein
   - die in § 29 BDSG aufgeführten Aufgaben wahrnehmen (z. B. eine Dateienübersicht aufstellen, die Mitarbeiter über den Sozialdatenschutz informieren usw.).

3. Keine Bedenken bestehen, wenn Bedienstete, die aufgrund des Erlasses des Hessischen Innenministers vom 2. Oktober 1978 bereits bisher die Aufgaben eines "kommunalen Datenschutzbeauftragten" wahrnehmen, auch diese Funktion nach § 79 SGB X mitübernehmen, sofern die unter 2. genannten Voraussetzungen erfüllt sind oder geschaffen werden. Auch in diesem Fall ist eine entsprechende zusätzliche schriftliche Bestellung notwendig.

Wegen der besonderen Bedeutung des Schutzes gerade der Sozialdaten sieht § 79 SGB X die Institutionalisierung einer innerbehördlichen Kontrolle des Datenschutzes - eben in Form der Bestellung eines mit dieser Aufgabe besonders betrauten Mitarbeiters - vor. Die Wichtigkeit dieser Maßnahme wird unterstrichen dadurch, daß das Gesetz die Nichtbestellung eines solchen Beauftragten als Ordnungswidrigkeit einstuft (vgl. den Verweis auf § 42 Abs. 1 Nr. 2 BDSG in § 79 Abs. 1 SGB X). Zu berücksichtigen ist auch hier wiederum, daß in der kommunalen Sozialverwaltung besonders schutzwürdige Daten verarbeitet werden. Nicht erbracht wurde bisher auch der Nachweis, inwiefern gerade die Besonderheiten der kommunalen Verwaltungsstruktur dazu führen, daß diese Bestellungspflicht - die den übrigen Sozialleistungsträgern kaum Probleme bereitet - in den Städten und Kreisen nicht durchgeführt werden könnte. Ein letztes Argument: Kommunen steht ebensowenig wie anderen Institutionen

eine "Verwerfungskompetenz" gegenüber Bundesgesetzen zu. Sollte der Bund, was den § 79 SGB X angeht, ohne Gesetzgebungskompetenz eine Angelegenheit des Verwaltungsverfahrens geregelt haben, steht die Feststellung der Verfassungswidrigkeit dieser Bestimmung nach der grundgesetzlichen Ordnung nur dem Bundesverfassungsgericht zu.

Auch in dieser Frage besteht Einigkeit unter den Datenschutzbeauftragten der Länder. Die Hessische Landesregierung hat in ihrer Antwort auf eine Kleine Anfrage im Hessischen Landtag vom 14. Oktober 1981 (Drucks. 9/5443) ebenfalls klargestellt, daß nach ihrer Auffassung die Bestellungspflicht in § 79 SGB X keinen unzulässigen Eingriff des Bundesgesetzgebers in das Kommunalrecht darstellt (Drucks. 9/5843). Jetzt liegt es an den Städten und Landkreisen, ihrer gesetzlichen Verpflichtung nachzukommen.

4.1.4
Sozialdatenschutz - Tendenzen der Entwicklung

Die weitere Entwicklung des Sozialdatenschutzes gilt es mit kritischer Aufmerksamkeit zu verfolgen. Es zeichnet sich eine Tendenz ab, das Sozialgeheimnis in verschiedenen Punkten wieder einzuschränken, sei es durch eine fragwürdige Interpretation der geltenden Bestimmungen - so etwa des § 79 SGB X durch die Verbände der Kommunen (dazu oben 4.1.3.2 und 4.1.3.3) -, sei es durch Bestrebungen, einzelne Vorschriften zu novellieren.

Diese Tendenz ist erklärlich. Zum einen handelt es sich - betrachtet man die weitreichende Bedeutung für die Verwaltungspraxis - bei dem 2. Kapitel des SGB X um ein vergleichsweise eilig beratenes und verabschiedetes Gesetz. Eine Reihe gravierender Anwendungsprobleme ist daher erst nachträglich erkannt worden. Zum anderen hat der abschließende Charakter des Katalogs zulässiger Übermittlungsfälle in §§ 67 ff. SGB X zur Konsequenz, daß eine Reihe seit langem etablierter Informationsströme zwischen Sozialbehörden und anderen Verwaltungszweigen unzulässig - weil nicht ausdrücklich erlaubt - ist.

Will man jedoch an der grundlegenden Absicht des Gesetzgebers mit dem SGB X, die Datenbestände der Sozialverwaltung prinzipiell gegenüber anderen Verwaltungszweigen abzuschotten, festhalten, sind Änderungswünsche mit dem Ziel einer Erweiterung der "Offenbarungsbefugnisse" für Sozialdaten mit äußerster Zurückhaltung zu betrachten. Daß triftige Gründe gegen eine Novellierung des § 79 SGB X im Sinne der von den Kommunen kritisierten Punkte (Behördenbegriff, Datenschutzbeauftragter) sprechen, habe ich soeben ausgeführt (vgl. 4.1.3.2, 4.1.3.3).

Der Sozialdatenschutz läuft weiterhin Gefahr, durch die folgende Entwicklung in Mitleidenschaft gezogen zu werden: Zunehmend knappere finanzielle Ressourcen für Ausgaben im Sozialbereich verstärken die Forderung nach mehr Kontrolle von Mißbräuchen bei der Inanspruchname von Leistungen - etwa der Sozialhilfe oder der Arbeitslosenversicherung. Der Ruf nach intensiverer Kontrolle gilt auch der Durchsetzung staatlicher Steueransprüche sowie den Beitragsverpflichtungen an die Sozialversicherung. Will man aber Beitragsehrlichkeit, vollständige Steuerzahlung und Korrektheit des Leistungsbezugs überwachen, erfordert dies eine Kooperation verschiedener Behörden, wobei sich diese Zusammenarbeit in erster Linie durch den Austausch personenbezogener Daten vollzieht. Jüngstes Beispiel hierfür ist das Gesetz zur Bekämpfung der illegalen Beschäftigung (BillBG) vom 15. Dezember 1981 (BGBl. I, S. 1390). Nach diesem Gesetz sollen sich u.a. Finanzämter, Arbeitsämter, Ordnungsämter und gesetzliche Krankenkassen gegenseitig unterrichten.

Meine Sorge gilt der Gefahr, daß eine solche Zusammenarbeit zu Kontrollzwecken zu einer übermäßigen Streuung von Sozialdaten führen kann, daß m.a.W. das Sozialgeheimnis durch Übermittlungserlaubnisse in Einzelgesetzen außerhalb des SGB X ohne zwingende Notwendigkeit durchlöchert werden könnte. Konsequenz muß sein, daß Richtung und Umfang solcher als Ausnahme erforderlicher Datenströme genau definiert und eng auf den jeweiligen Gesetzeszweck bezogen werden. Zwar enthält das BillBG eine Beschränkung des Informationsaustausches auf den Einzelfall, doch widerspricht es der hier aufgestellten Forderung, wenn im Zusammenhang mit der Verabschiedung dieses Gesetzes auch die Norm des § 71 Nr. 3 SGB X über die Mitteilungspflichten an die Finanzämter erweitert wird, ohne daß eine Eingrenzung auf den Gesetzeszweck erfolgt ist. Ich habe die zuständigen Bundestagsausschüsse im Zuge des Gesetzgebungsverfahrens - leider ohne Erfolg - hierauf hingewiesen.

4.2
Geheimhaltung und innerbehördliche Kommunikationschranken - Auswirkungen der Berufsgeheimnisse auf den innerdienstlichen Informationsaustausch

4.2.1
Das Problem

Eine Reihe von Anfragen und Eingaben bezog sich 1981 auf das Problem der sog. "innerbehördlichen Schweigepflicht". Diese Frage wird unter Praktikern der Sozialarbeit intensiv debattiert, hat jedoch bisher in der allgemeinen Datenschutzdiskussion noch kaum Beachtung gefunden. Dabei geht es um die Frage, welche Konsequenz und Reichweite die in § 203 Abs. 1 Strafgesetzbuch (StGB) statuierte Geheimhaltungspflicht des Sozialarbeiters, des Psychologen oder des Mitarbeiters von Beratungsstellen im innerdienstlichen Informationsverkehr der Sozialbehörden hat; ob sie dazu verpflichtet, personenbezogene Angaben der Klienten nicht nur gegenüber außenstehenden Dritten - das ist unbestritten -, sondern unter bestimmten Umständen auch gegenüber Kollegen, Vorgesetzten, Aufsichtsbehörden oder Prüfungsgremien geheimzuhalten. Im Hintergrund dieser Fragestellung stehen unterschiedliche Auffassungen über die Stellung und Rolle der Sozialarbeit im Gesamtsystem staatlicher Sozialpolitik sowie über die Notwendigkeit "informationeller Abschottung" im Interesse klientelorientierter Sozialbetreuung.

Aktuelle Anlässe dieser Anfragen waren z.B.

- die Aufforderung des Leiters eines Jugendamts an die - diesem Amt organisatorisch angegliederte - Erziehungsberatungsstelle, ihm Akten über Beratungsfälle vorzulegen;
- das Verlangen einer Prüfungskommission an einen Schulpsychologen, ihr Einsicht in die Unterlagen von begutachteten Schülern zu gewähren;
- die mit einer Dienstanweisung an alle Sozialarbeiter einer Kommune verfügte Pflicht, ausnahmslos jeden Klientenkontakt aktenmäßig festzuhalten.

In allen drei Fällen äußerten die betroffenen Mitarbeiter unter Berufung auf ihre Schweigepflicht Bedenken gegen die Aktenweitergabe an bzw. Einsichtnahme durch Dritte.

Diese Einzelfälle signalisieren ein grundlegendes Problem öffentlich-rechtlich organisierter Sozialarbeit: das Spannungsverhältnis zwischen notwendiger Informationsweitergabe zur Durchführung bzw. Abwicklung von Sozialleistungen einerseits und der Diskretion und Verschwiegenheit des einzelnen Sozialarbeiters andererseits, die Voraussetzung für ein Vertrauensverhältnis zum ratsuchenden Bürger sind. Die öffentliche Sozialverwaltung liefert, besonders in den Kommunen, vielfach ein Hilfe- und Beratungsangebot, das dem der freien Wohlfahrtsverbände entspricht; das gilt etwa für die Familien-, Erziehungs- und Drogenberatung. Bei dieser Tätigkeit spielt die persönliche Vertrauensbeziehung zwischen Berater und Klienten eine zentrale Rolle. Der Klient legt seine Intimsphäre offen in der Erwartung strikter Vertraulichkeit. Auf der anderen Seite ist der einzelne Mitarbeiter des Sozialamts oder des Jugendamts, anders als sein Kollege bei einem freien Träger, Teil einer Behörde. "Behörde" aber steht für formalisierte Verwaltungsverfahren, für hierarchische Kontrolle, für eine Einheit, die intern keine informationellen Freiräume vorsieht oder duldet. Sind Daten erst einmal in eine Behörde gelangt, stehen sie dort für die breite Palette der gesetzlichen Aufgaben zur Verfügung; andere Behörden können grundsätzlich im Wege der Amtshilfe auch für andere Verwaltungszwecke auf diese Datenbestände zugreifen.

Die Aufgaben der Sozialbehörden führen unter Umständen zu einer Reihe von Maßnahmen, die in die Sphäre des Bürgers eingreifen und ggf. auch gegen seinen Willen durchgeführt werden können. Am Beispiel demonstriert: Der Ratsuchende, der in der Sprechstunde eines freien Wohlfahrtsverbandes seine Erziehungsprobleme diskutiert, kann der Vertraulichkeit des Gesprächs sicher sein. Muß er aber, wenn er das gleiche gegenüber einem Mitarbeiter des Jugendamtes tut, damit rechnen, daß unter Umständen eine Fürsorgeerziehung eingeleitet wird? Diese Divergenz läßt das Problem genauer orten, das auf der juristischen Ebene zur Diskussion um die "innerbehördliche Schweigepflicht" führt: Die traditionellen Bedingungen administrativer Informationsverarbeitung und -nutzung entsprechen nicht den besonderen Funktionsvoraussetzungen beratender und betreuender Sozialarbeit.

4.2.2
Rechtliche Lösungsansätze

Der Gedanke, daß auch innerhalb von Verwaltungseinheiten, d.h. zwischen verschiedenen Mitarbeitern der gleichen Behörde, Datenbestände funktionsbezogen abgeschottet werden, ist nicht neu. So beinhaltet beispielsweise der Grundsatz der Vertraulichkeit von Personalakten seit jeher, daß persönliche Daten der Bediensteten nur den mit der Personalsachbearbeitung betrauten Mitarbeitern zugänglich sein dürfen. Die Datenschutzgesetze enthalten mit der Konstruktion des "Datengeheimnisses" das informationelle Strukturprinzip, daß personenbezogene Daten auch innerhalb speichernder Stellen (Behörden, Unternehmen) nur zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck - der durch den Dienst- oder Organisationsplan, durch die Geschäftsverteil-

lung usw. konkretisiert wird - bekanntzugeben, zugänglich zu machen oder sonst zu nutzen sind. Die neuen Vorschriften über das Sozialgeheimnis im Zehnten Buch des Sozialgesetzbuchs (§§ 67 ff. SGB X) sind dagegen für die juristische Bewältigung des geschilderten Problems nicht einschlägig: Sie regeln und begrenzen die Weitergabe von Sozialdaten durch "Sozialleistungsträger", sind also an die Behörde oder Körperschaft adressiert.

Die Geheimhaltungspflicht des § 203 Abs. 1 StGB jedoch trifft jedes Mitglied der in dieser Vorschrift genannten Berufsgruppen (etwa Ärzte, Rechtsanwälte, Berufspsychologen, Mitarbeiter staatlich anerkannter Beratungsstellen usw.) wie jede Strafrechtsnorm persönlich. Die Berufsgeheimnisse gelten zunächst unabhängig davon, ob der Betroffene freiberuflich tätig ist oder als Arbeitnehmer oder Beamter in eine Behördenorganisation eingebunden ist. Keine Rolle spielt die gleichzeitige Eigenschaft als "Amtsträger" im Sinne des Abs. 2 des § 203, der den Geheimnisschutz für die Datenweitergabe im Wege der Amtshilfe ausschließt. Dennoch besteht ein wichtiger Unterschied: Geht man davon aus, daß beispielsweise der Klient der Sozialverwaltung seine Angaben, die Geheimnisse enthalten, der Behörde oder dem Amt als solchem, nicht aber einem bestimmten Amtsträger gegenüber macht und auch im letzteren Fall sein Vertrauen nicht dem Bediensteten in Person, sondern als Repräsentanten der Sozialbehörde entgegenbringt ("funktionales Vertrauen"), greift § 203 Abs. 1 StGB für die juristische Bewertung der Zirkulation der "Geheimnisse" innerhalb dieser Behörde nicht ein. Werden Informationen von vornherein für einen bestimmten Personenkreis gegeben, sind diese Personen untereinander keine tauglichen Täter im Sinne des § 203 Abs. 1 StGB, weil sie der Informationsgeber gleichermaßen zum Vertrauensträger gemacht hat.

Anders jedoch dann, wenn Grundlage für die Mitteilung von Geheimnissen erkennbar die Vertrauensbeziehung zu einem bestimmten Behördenangehörigen ist, insbesondere wenn dieser zugleich Inhaber einer besonderen Vertrauensstellung im Sinne der in § 203 Abs. 1 genannten Berufsgeheimnisse ist. In dieser Konstellation bedeutet auch die Weitergabe durch diesen Mitarbeiter an einen Kollegen oder Vorgesetzten ein "Offenbaren" im Sinne der genannten Bestimmung, das keineswegs allein durch das dienstrechtliche Verhältnis gerechtfertigt ist. Die Gehorsamspflicht aus dem Dienst- oder Arbeitsverhältnis alleine vermag in diesen Fällen die Geheimhaltungspflicht des Sozialarbeiters, Berufspsychologen, Ehe- oder Jugendberaters etc. nicht zu durchbrechen; vielmehr muß als Legitimation für eine Offenbarung eine gesetzliche Mitteilungspflicht oder einer der anerkannten Rechtfertigungsgründe des Strafrechts vorliegen.

Es ist nicht einfach, in Anbetracht des umfassenden fürsorgerischen Auftrags der Sozialverwaltung besonders im Bereich der Sozial- und Jugendhilfe und angesichts der Vielfalt ihrer ineinandergreifenden Aufgaben und Befugnisse eine klare Grenze zwischen dem Sozialarbeiter, Psychologen usw. in seiner Rolle als Behördenangehöriger einerseits und als Partner einer kommunikativen Zweierbeziehung mit dem Klienten andererseits zu ziehen. Vieles hängt hier vom Einzelfall ab, etwa von der Stellung des einzelnen Mitarbeiters in der Informations- und Entscheidungshierarchie der Sozialbehörde und von seiner genauen Aufgabenstellung. Für den Bereich der Sozial- und Jugendhilfe ist angeregt worden, zwischen der Mitwirkung an Verwaltungsverfahren bei der Abwicklung von Sach-und Geldleistungen (Behördenfunktion) und der auf persönlicher Beziehung zum Klienten basierenden Interaktion (dann auch "innerbehördlich" Schweigepflicht) zu unterscheiden. Diese Ansätze bedürfen noch weiterer Präzisierung, um die Reichweite der Berufsgeheimnisse von Behördenbediensteten klar definieren zu können. Problematisch erscheint dies insbesondere deshalb, weil bei vielen Mitarbeitern der Sozialverwaltung beide Tätigkeiten schwer trennbar miteinander verknüpft sind.

Dennoch gibt es Bereiche, in denen sich Konturen klarer abzeichnen, in denen das individuelle Anvertrauen von Geheimnissen so eindeutig im Vordergrund steht, daß Konsequenzen aus dem Berufsgeheimnis auch für den innerdienstlichen Verkehr mit Informationen unvermeidlich sind. Zwei dieser Berufsgruppen werden im folgenden herausgegriffen: die Mitarbeiter von Beratungsstellen und die Schulpsychologen.

4.2.3
Konsequenzen für einzelne Berufsgruppen

4.2.3.1
Die Geheimhaltungspflicht der Mitarbeiter von Beratungsstellen

Eindeutig institutionell abgrenzbar im Sinne eines abzuschottenden "informationellen Freiraums" sind die Beratungsstellen für Ehe-, Erziehungs-, Jugend- und Drogenprobleme. Auch wenn sie von Kommunen oder sonstigen öffentlichen Stellen betrieben werden, muß die Beratung und Betreuung unter den gleichen Arbeitsbedingungen stattfinden können wie bei freien Trägern. Dazu gehört aber auch die sichere Erwartung des Ratsuchenden, daß strikte Vertraulichkeit gewahrt wird, auch in dem Sinne, daß seine persönlichen Daten nicht zu anderen, etwa administrativen Zwecken, verwandt werden. Die staatliche Organisation dieser Stellen darf nicht dazu führen, daß der hilfesuchende Bürger mit seinen Problemen verwaltet wird. Die öffentlich-rechtliche Trägerschaft ebenso wie die organisatorische Anbindung an Behörden oder Ämter dürfen daher hinsichtlich der Einhaltung der Schweigepflicht keinen Unterschied machen. Diesem Postulat entspricht es, wenn die hessischen Richtlinien sowohl für

Erziehungsberatungsstellen (StAnz. 51/1980 S. 2391) als auch für Jugend- und Drogenberatungsstellen (StAnz. 1/1981 S. 35) Aufgaben, Tätigkeiten, Arbeitsweise und Ausstattung unabhängig von der Trägerschaft gleich regeln. Die Erziehungsberatungsstelle arbeitet nach diesen Richtlinien "in eigener Verantwortung" (Nr. 4.3), "sie soll getrennt von den Räumen einer Behörde... untergebracht sein" (Nr. 7.2), Verbindung wegen eines bestimmten Klienten zu Sozial-, Jugend- und Gesundheitsamt soll sie nur mit Zustimmung des Ratsuchenden aufnehmen (Nr. 8.5).

Diese konkreten Anforderungen aus fachlicher Sicht unterstreichen, was die Sammlung und Nutzung personenbezogener Angaben angeht, exemplarisch die Notwendigkeit, diese Stellen vom Datenbestand auch derjenigen Ämter und Behörden, denen sie an- oder in die sie eingegliedert sind, abzutrennen. Konkret: Mitarbeitern dieser Stellen erlegt § 203 Abs. 1 Nr. 4 und 4a StGB auch "innerbehördlich" eine Geheimhaltungspflicht auf, weil ihnen "zum persönlichen Lebensbereich gehörende Geheimnisse" individuell anvertraut worden sind. Die Weitergabe einzelner Mitteilungen, erst recht von Gutachten oder Akten, bedarf der Zustimmung des Klienten oder eines besonderen Rechtfertigungsgrundes (z.B. gesetzliche Mitteilungspflicht, übergesetzlicher Notstand usw.). Damit nicht zu verwechseln ist die Frage, ob der Betroffene in bestimmten Fällen dazu verpflichtet ist, seine Einwilligung zu geben, damit eine Sozialbehörde den Anspruch auf beantragte Sozialleistungen überprüfen kann (vgl. dazu §§ 60 ff. SGB I über die Mitwirkungspflicht).

4.2.3.2
Das Berufsgeheimnis der Schulpsychologen

4.2.3.2.1
Der aktuelle Konflikt

Der Erlaß einer neuen Dienstordnung für Schulpsychologen durch den Hessischen Kultusminister steht kurz bevor. Die Notwendigkeit für diese Neuregelung entstand, nachdem ein Diplom-Psychologe sich bei mir beschwert hatte. Er war der Auffassung, daß seine Schweigepflicht nach Nr. 2 des § 203 Abs. 1 ("Berufspsychologen") dadurch verletzt werde, daß er dem Prüfungsausschuß, der auf Grund der Ziff. IV der "Richtlinien für die Einarbeitung von Diplom-Psychologen - ohne vollpädagogische Ausbildung - in ihre Tätigkeit im schulpsychologischen Dienst" (Erlaß des Hessischen Kultusministers vom 17. August 1971, Amtsblatt S. 727) beim Hessischen Kultusminister besteht, Einblick in seine vollständigen Klientenakten gewähren solle. Das Erfordernis einer Überprüfung der psychologischen Einzelfallarbeit und einer korrekten Aktenführung stand dabei zu keiner Zeit zur Debatte. Vielmehr hat der betroffene Schulpsychologe ein Verfahren vorgeschlagen, das seiner Meinung nach der ihm obliegenden Geheimhaltungspflicht genügte und zugleich eine Überprüfung der fachlichen Eignung ermöglichte. Im Gegensatz dazu bestand der Prüfungsausschuß bei der Überprüfung in der Dienststelle des Petenten auf vollständiger Akteneinsicht. Auch das Angebot, eine Akte nach Wunsch des Ausschusses in dessen Gegenwart auszuwählen, zu fotokopieren und die personenbezogenen Einzelangaben zu schwärzen, wurde abgelehnt; der Prüfungsausschuß hat daraufhin die Überprüfung abgebrochen.

Der Hessische Kultusminister hat in einem Schreiben an den Petenten auch zur Frage der "innerbehördlichen Schweigepflicht" Stellung genommen. Insbesondere vertrat er die Ansicht, daß der Prüfungsausschuß in die von dem Psychologen geführten Unterlagen deshalb Einsicht nehmen müsse, um festzustellen, ob dieser seine Beratung "lege artis" durchführe. Er hat hierzu wörtlich ausgeführt: "Hierbei ist der Name eines Probanden ohne Bedeutung". Die Anonymität der Klienten werde nicht in Frage gestellt, weil die Ausschußmitglieder selbst der Schweigepflicht unterlägen. Es sei daher von der mutmaßlichen Einwilligung des Probanden darin auszugehen, daß das, was dieser dem Psychologen anvertraut hätte, auch den der Schweigepflicht unterliegenden Mitgliedern des Prüfungsausschusses bekannt werde.

4.2.3.2.2.
Die rechtliche Beurteilung

4.2.3.2.2.1
Stellungnahme zum Einzelfall

Dieser Auffassung des Kultusministers habe ich aus folgenden Gründen widersprochen:

Der Hessische Kultusminister geht zunächst in den genannten Richtlinien selbst davon aus, daß die fachliche Eignung von Diplom-Psychologen auch ohne Akteneinsicht durch den Prüfungsausschuß festgestellt werden kann; die Überprüfung nach der 18-monatigen Einarbeitungszeit beschränkt sich auf eine schriftliche Arbeit und ein Fachgespräch. Selbst wenn die Richtlinien die Vorlage von Beratungsunterlagen verlangen würden, wäre dies unbeachtlich, da bloße Verwaltungsvorschriften keine hinreichende Rechtsgrundlage für eine Geheimnisoffenbarung darstellen können, weil sie keine Eingriffsbefugnisse in strafrechtlich geschützte Rechtsgüter schaffen können.

Die "mutmaßliche Einwilligung" schied als Rechtfertigungsgrund deshalb aus, weil sie voraussetzt, daß der Geheimnisträger (hier: der Schulpsychologe) glaubt, im vermeintlichen Interesse der Probanden zu handeln. Gerade dies hatte aber der Petent nicht angenommen, sondern vielmehr das Interesse seines Klienten nur durch die Geheimhaltung seiner Daten gewahrt gesehen. Die Tatsache, daß auch der Empfänger der Mitteilung (hier: die Mitglieder des Prüfungsausschusses) einer Schweigepflicht unterliegen, rechtfertigt alleine ebenfalls nicht die Annahme, daß die Betroffenen mit der Einsicht Dritter in ihre Unterlagen stillschweigend einverstanden sind. Die Fiktion eines "Schweigepflichtverbundes" aller Träger von Berufsgeheimnissen mit der Konsequenz intern unbeschränkten Datenaustauschs ist im übrigen weder mit § 203 StGB noch mit den Datenschutzgesetzen in Einklang zu bringen.

4.2.3.2.2.2
Rechtliche Grundsätze für eine generelle Regelung

Der Kultusminister hat sich inzwischen nicht nur meiner Beurteilung der Rechtslage im Einzelfall angeschlossen, sondern eine allgemeine Regelung der "innerbehördlichen Schweigepflicht" für Schulpsychologen als erforderlich angesehen. Dafür habe ich folgende Kriterien vorgeschlagen:

4.2.3.2.2.2.1
Notwenddigkeit der Aufgabendifferenzierung

Die Dienstordnung muß deutlich machen, wo die Grenzen der strafrechtlichen Geheimhaltungspflicht des Berufspsychologen im Schuldienst - auch gegenüber weisungsbefugten Fachbeamten - verlaufen. Die Aufgabendefinition muß geeignet sein, hierfür Abgrenzungskriterien zu vermitteln. Nach Art. 56 der Hessischen Verfassung i.V.m. Art. 7 GG hat die Schule neben einem allgemeinen Bildungsauftrag auch eine Erziehungsaufgabe, die sie gemeinsam mit den Eltern erfüllt, denen nach Art. 6 GG "zuvörderst" die Erziehung ihrer Kinder obliegt. Hieraus ergibt sich ein Spannungsverhältnis zwischen elterlicher und schulischer Erziehungsgewalt, das nur in der jeweiligen Einzelfallentscheidung seine Auflösung finden kann. Der aus Art. 6 Abs. 2 GG ableshare grundsätzliche Vorrang der prinzipiell umfassenderen elterlichen Erziehungsgewalt findet insofern im schulischen Bereich eine Begrenzung; hier ist der staatliche Erziehungsauftrag dem elterlichen gleichgeordnet (vgl. BVerfGE 34, 165 ff.).

Konsequent nennt auch die derzeit geltende Dienstordnung für Schulpsychologen (Erlaß vom 18. August 1971 -E IV 4 - 1011/210 - 32 -) bei den Aufgaben des § 3 neben rein schulisch-institutionellen Unterstützungstätigkeiten auch und gerade die "Individualberatung" (vgl. § 3 Ziff. I 1; im einzelnen z.B. "Anhörung und Beratung von Schülern, Eltern und Lehrern in Konfliktfällen", Ziff. I 3; Beratung von "Erziehungsberechtigten", Ziff. I A 1 und 2). In diesem Zusammenhang besonders hervorzuheben ist die "Beratung bei alterstypischen Verhaltensauffälligkeiten, z.B. bei Entwicklungsstörungen, sexuellen Problemen, Autoritätskonflikten, Jugendkriminalität, Rauschmittelgebrauch und neurotischen Störungen" (vgl. § 3 II B Ziff. 6).

Aus diesen klientelorientierten Aufgaben des Schulpsychologen folgt, daß seine Tätigkeit sich zwar im Sinne eines verfassungsrechtlich verbürgten Bildungs- und Erziehungsauftrages der Schule vollzieht, aber z.T. weit über den institutionellen Aspekt von Schule hinausgeht, der im Schulverwaltungsgesetz und im Schulpflichtgesetz geregelt ist. Sie umfaßt daher gleichberechtigt - wie dies auch in der Dienstordnung zum Ausdruck kommt - die Unterstützung des staatlichen und des elterlichen Erziehungsauftrags.

4.2.3.2.2.2.2
Beschränkung der Fachaufsicht

Zweifelsfrei ist, daß diese individuell beratende Tätigkeit aus verfassungsrechtlichen Gründen keiner Fachaufsicht insoweit unterliegt, als sie das allgemeine Persönlichkeitsrecht von Schulbenutzern im Sinne von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG tangiert. So kann aus der Formulierung von Art. 7 GG, daß das gesamte Schulwesen unter der "Aufsicht" des Staates stehe, nicht geschlossen werden, es handele sich dabei um die klassische Fach- oder Rechtsaufsicht der öffentlichen Verwaltung. Die Schulaufsicht im Sinne des Art. 7 Abs. 1 GG ist vielmehr nach gefestigter Auffassung in Rechtsprechung und Lehre und ihrer Ausformulierung in einzelnen Länderverfassungen ein aus seiner geschichtlichen Entstehung heraus weit auszulegender Sammelbegriff, der die Gesamtheit der Rechte und Pflichten des Staates zur äußeren und inneren Gestaltung des Schulwesens einschließlich der Aufsicht im engeren Sinne umfaßt (vgl. BVerfGE 26, 228 ff.; 34, 165 ff.; BVerwGE 18, 38 ff.). Die geltende Dienstordnung für Schulpsychologen sieht daher auch - anders als der mir vorgelegte Erlaß-Entwurf - folgerichtig vor, daß der Schulpsychologe im Hinblick auf den sachlichen Inhalt seiner Tätigkeit an Weisungen nicht gebunden ist (§ 9 Abs. 2), mithin insoweit keiner Fachaufsicht unterliegt.

Die Wahrung des Berufsgeheimnisses erfordert also eine Differenzierung in primär klientelorientierte Funktionen der Schulpsychologen und solche, die die Institution Schule unterstützen (z.B. Maßnahmen nach §§ 3 bis 6 Schulpflichtgesetz, Beratung von Lehrern, Durchführung von Tests), eine Abgrenzung zwischen Tätigkeiten innerhalb des staatlichen Schulwesens aufgrund von Gesetzen einerseits und solchen Leistungen andererseits, die der Schulpsychologe aufgrund freiwilliger Mitwirkung von Schulbenutzern erbringt.

Die Konsequenz ist die Beschränkung der staatlichen Schulaufsicht in der Abteilung "Schulpsychologischer Dienst" auf die bloße Rechtsaufsicht bei der Aufgabenerfüllung außerhalb gesetzlicher Verpflichtungen, während für einige schulunterstützende Tätigkeiten auf gesetzlicher Grundlage sowohl Fach- als auch Rechtsaufsicht gegeben sein müssen. Dies gilt insbesondere für die Beteiligung von Schulpsychologen an Verwaltungsverfahren im Sinne des Hessischen Verwaltungsverfahrensgesetzes.

4.2.3.2.2.2.3
Gesetzesvorbehalt im Schulverhältnis

Die Grundrechtsverwirklichung des Schülers muß der Maßstab auch für schulorganisatorische Maßnahmen sein und in ihnen zum Ausdruck kommen. Die Offenbarung zum persönlichen Lebensbereich gehörender Geheimnisse des Schülers bzw. des Erziehungsberechtigten aus den Akten des einzelnen Schulpsychologen gegenüber der staatlichen Schulaufsicht ist ein Eingriff in das grundrechtlich geschützte Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) dieser beiden Personengruppen. Da Grundrechtseinschränkungen, soweit überhaupt zulässig, der gesetzlichen Grundlage bedürfen, muß Schulrecht überall dort gesetzlich oder auf Grund gesetzlicher Ermächtigung ergehen, wo die Normen innerhalb des Schulverhältnisses Grundrechte der Schulbenutzer tangieren. Das Bundesverfassungsgericht hat die Notwendigkeit des Gesetzesvorbehaltes für die Fälle wesentlicher Betroffenheit der Schulbenutzer betont (vgl. zur "Wesentlichkeitstheorie" insbesondere BVerfGE 33, 303, 337 und 34, 165 ff., 192 ff. "Hessische Förderstufe").

4.2.3.2.3
Ergebnis: Neue Dienstordnung für Schulpsychologen

Der Kultusminister hat inzwischen einen Entwurf für "Richtlinien für die Tätigkeit der Schulpsychologen in der Abteilung Schulpsychologischer Dienst" vorgelegt, der die von mir geforderte funktionelle Differenzierung der Aufgaben enthält und demnächst in Kraft treten soll (auszugsweise wiedergegeben unter 5.3).

4.2.4
§ 203 StGB - kein informationelles Strukturprinzip für die Sozialverwaltung

Die Ausführungen der vorigen Abschnitte haben deutlich gemacht, daß sich zwar das Grundprinzip zur Fundierung einer auch "innerbehördlich" wirkenden Geheimhaltungspflicht aus § 203 StGB herausarbeiten läßt: die Scheidelinie verläuft zwischen der Einzelfallberatung als Hilfestellung zur Lebensbewältigung - mit der Konsequenz, daß Geheimnisse individuell "anvertraut" werden - einerseits und dem Verwaltungsvollzug zur Erbringung von Sozialleistungen andererseits.

Nicht ohne Grund sind jedoch die Anwendungsvoraussetzungen und Auswirkungen dieses Prinzips auf zwei Berufsgruppen (Mitarbeiter von Beratungsstellen in 4.2.3.1, Schulpsychologen in 4.2.3.2) so eingehend dargestellt worden. Damit wird aufgezeigt, daß die Konkretisierung dieses Grundsatzes im Hinblick auf den Aufgabenbereich des einzelnen Behördenbediensteten eine Fülle von verfassungs-, straf-, dienst- und datenschutzrechtlichen Erwägungen notwendig machen kann. Dabei wäre es verfehlt, ausgerechnet vom Strafrecht, also vom Ansatz bei der möglichen Strafbarkeit des betroffenen Sozialarbeiters Patentlösungen oder auch nur hinreichende Vorgaben für eine Informationsstruktur der Sozialverwaltung zu erwarten, die den Bedingungen moderner Sozialarbeit gerecht wird. Über den Aspekt "innerbehördliche Schweigepflicht" können die Probleme der Berufsrollendefinition der Sozialarbeiter nicht erschöpfend gelöst werden.

Diese Feststellung wird erhärtet durch die folgenden Bemerkungen:

- § 203 StGB schützt sowohl den einzelnen Klienten vor der Preisgabe seiner Privatsphäre als auch das allgemeine Vertrauen der Öffentlichkeit in die Verschwiegenheit bestimmter Berufsgruppen. Die Vorschrift enthält jedoch nur ein aus dem Geheimhaltungsinteresse des Betroffenen abgeleitetes, kein originäres Schweigerecht von Sozialarbeitern usw. Eine Gewährleistung dahingehender "standespolitischer" Forderungen läßt sich dieser Bestimmung mithin nicht entnehmen.

- Die Dogmatik der Rechtfertigungsgründe zu § 203 StGB - also der Situationen, in denen eine Weitergabe persönlicher Angaben zulässig ist - birgt viele rechtliche Unsicherheiten. Dies gilt nicht nur für die sog. "stillschweigende" bzw. "mutmaßliche" Einwilligung des Betroffenen, sondern erst recht für den Grundsatz der Güter- und Interessenabwägung (§ 34 StGB), dessen Konkretisierung gerade bei den Geheimschutzdelikten noch in den Anfängen steckt, sicher aber nicht ohne Beachtung der Prinzipien der Datenschutzgesetze erfolgen darf.

- Während bestimmte in § 203 Abs. 1 StGB genannte Berufsgruppen - wie etwa die Ärzte oder Rechtsanwälte -über ein kodifiziertes Berufs- bzw. Standesrecht verfügen, das Geltung und Reichweite des Berufsgeheimnisses konkretisiert, trifft dies gerade für die im Sozialbereich Tätigen (Sozialarbeiter, Psychologen etc.) nicht zu. Der gleiche Unterschied gilt, was die Einräumung eines Zeugnisverweigerungsrechtes vor Gericht angeht.

Auch wenn im Einzelfall die Voraussetzungen für eine "innerbehördliche Schweigepflicht" vorliegen, heißt dies keineswegs, daß sich die Arbeit der geheimhaltungspflichtigen Behördenbediensteten im kontrollfreien Raum abspielt. Überprüfungen und Leistungsbeurteilungen durch Vorgesetzte und Prüfungsinstanzen, die auf Personenbezug verzichten (z.B. Fallstatistiken), können arbeits- bzw. dienstrechtliche Probleme aufwerfen; Geheimnis- und Datenschutz jedenfalls greifen hier nicht ein.

4.2.5
Konsequenzen

Die hier angestellten Erwägungen beruhen auf einer Reihe von Gesprächen mit Mitarbeitern von Sozialbehörden auf verschiedensten Ebenen (Vorgesetzte, Amtsleiter, Sozialarbeiter usw.), mit sachverständigen Hochschullehrern und anderen betroffenen Berufsgruppen. Sie stellen einen Einstieg in die Problematik dar und sollen die weitere Diskussion anregen. Für das kommende Jahr beabsichtige ich, die Gesprächsserie fortzusetzen, um zu weiteren Konkretisierungen zu gelangen. Von den Sozialleistungsträgern und Aufsichtsbehörden muß allerdings schon jetzt erwartet werden, daß sie die innerdienstlichen Auswirkungen der Berufsgeheimnisse bei der Abfassung von Erlassen sowie beim Erlaß von Dienstordnungen, Hausverfügungen oder Geschäftsanweisungen, also bei jeder Regelung des innerbehördlichen Informationsaustauschs berücksichtigen.

4.3
Datenaustausch innerhalb der Gemeinde:
Informationseinheit oder Übermittlungsschranken?

Auch zunächst rein theoretisch anmutende Streitfragen um die Interpretation einzelner Bestimmungen der Datenschutzgesetze können rasch praktische Bedeutung gewinnen. Insbesondere die Auslegung der Schlüsselbegriffe - hierzu zählen u.a. "Übermittlung" und "speichernde Stelle" - sorgen immer wieder für aktuelle Kontroversen mit wichtigem Praxisbezug. Ein Beispiel hierfür ist die Diskussion um die datenschutzrechtliche Struktur der Gemeinden, an der sich derzeit vor allem die kommunalen Spitzenverbände intensiv beteiligen.

Ausgangspunkt ist die Funktion der Übermittlungsvorschriften der Datenschutzgesetze im öffentlichen Bereich: Ein wesentliches Element des Datenschutzes ist die Beschränkung der Weitergabe von Daten zwischen öffentlichen Stellen. Nur dann, wenn eine der beiden beteiligten Stellen für die Erfüllung ihrer Aufgaben auf die Datenweitergabe angewiesen ist, darf diese auch erfolgen. Diese rechtliche Schranke ist Ausdruck des Grundsatzes, daß jede öffentliche Stelle nur die Daten erhalten und verarbeiten soll, die sie auch wirklich benötigt. Das Gesetz schließt aber nicht nur ungehinderte Datenströme aus, es verpflichtet auch die beiden Partner des Datentransfers dazu, jeweils vor der Übermittlung zu prüfen, ob diese Voraussetzungen auch gegeben sind.

Insbesondere bei Verwaltungseinheiten, die große und komplexe Aufgabenbereiche wahrnehmen, taucht immer wieder die Frage auf, ob auch der Datenaustausch zwischen einzelnen Abteilungen, die unterschiedliche Aufgaben erfüllen, den Übermittlungsvorschriften der Datenschutzgesetze unterliegt. Nimmt man als Beispiel die Kommune, wird die praktische Relevanz dieses Problems aus der folgenden alternativen Fragestellung deutlich: Kann der Datenaustausch zwischen verschiedenen Ämtern der selben Kommunalverwaltung ohne Beachtung der einengenden Zulässigkeitsvoraussetzungen der Übermittlung erfolgen? Oder sind auf eine solche Weitergabe - etwa aus dem Ausländeramt an das Sozialamt - die Übermittlungsvorschriften ohne Einschränkung anzuwenden?

Sieht man die Gemeinde datenschutzrechtlich als Einheit, müßte man letztere Frage verneinen. Die Datenschutzgesetze fordern indes eine andere Konzeption: Jede Gemeinde muß in ihrem Anwendungsbereich als ein zusammengefaßter Bestand einer Vielzahl einzelner "speichernder Stellen" angesehen werden, die jeweils eine bestimmte Funktion wahrnehmen, zwischen denen aber die gesetzlichen Übermittlungsschranken zu beachten sind. Die Gesetze gehen somit von einem "funktionalen Stellenbegriff" aus.

Ausgangspunkt dieses Verständnisses vom Begriff der "speichernden Stelle" ist der Wortlaut der Datenschutzgesetze. So folgt aus der Formulierung von § 7 Abs. 2 Nr. 1 BDSG bzw. § 3 Abs. 1 HDSG, daß die Gemeinden **mehrere** speichernde Stellen haben. Diese Vorschriften sprechen von den "öffentlichen Stellen (....) der Gemeinden" in der Mehrzahl. In einem wichtigen Bereich der gemeindlichen Aufgabenerfüllung gibt es seit kurzem eine Norm, die sich eindeutig zum "funktionalen Stellenbegriff" bekennt: Nach § 18 Abs. 6 des Melderechtsrahmengesetzes vom 22. August 1980 sind die Übermittlungsvorschriften dieses Gesetzes auf die Weitergabe von Daten aus dem Einwohnermelderegister an andere gemeindliche Abteilungen anzuwenden. Die Mitteilung solcher Meldedaten etwa an das kommunale Steueramt ist somit nur unter den Bedingungen der Übermittlungsvorschriften zulässig. Es ist zu erwarten, daß das künftige Hessiche Meldegesetz diese Vorschrift ebenso übernehmen wird wie die neu zu erlassenden Meldegesetze der anderen Bundesländer. Es ist wenig sinnvoll, das Meldeamt von den übrigen Teilen der Gemeinde zu trennen und datenschutzrechtlich besonderen Regeln zu unterwerfen.

Nicht nur der Wortlaut, sondern auch - ja vor allem - der Zweck der Datenschutzgesetze unterstreicht die Geltung des "funktionalen Stellenbegriffs". Sowohl das Bundesdatenschutzgesetz als auch die Landesdatenschutzgesetze haben die Systematik der Weitergabe von Daten öffentlicher Stellen abschließend geregelt. Für den öffentlichen Bereich sind die Vorschriften der §§ 12, 16 HDSG bzw. 10, 11 BDSG heranzuziehen; außerdem sind § 9 HDSG bzw. § 5 BDSG (Datengeheimnis) zu berücksichtigen. Beide Normenbereiche regeln die Weitergabe von Daten abschließend. Die Vorschriften über das Datengeheimnis untersagen es den bei der Datenverarbeitung beschäftigten Personen, "geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu (...) nutzen". Die Zweckbindung der Datenverarbeitung kann sich jedoch immer nur auf den konkreten Zweck beziehen, der für die Speicherung und Weiterverarbeitung der Daten gegeben ist. Personalausweisdaten dienen der rechtmäßigen Ausstellung und Verwaltung von Ausweisen und stehen keinesfalls als "Kommunaldaten" allen kommunalen Abteilungen zur Verfügung.

Als Ausnahme im Verhältnis zu diesem generellen Verbot zweckwidriger Nutzung begründen die Übermittlungsnormen die Befugnis, Daten auch zu anderen Zwecken als denen, die der ursprünglichen Speicherung zugrundeliegen, weiterzugeben. Diese Ausnahme gilt jedoch nur dann, wenn - wie schon mehrfach betont - die Weitergabe zur rechtlich festgelegten Aufgabenerfüllung einer der beiden beteiligten Stellen erforderlich ist. Dieses "Verbot mit Erlaubnisvorbehalt" kennt keinen anderen zulässigen Datentransfer als eben die gesetzlich geregelte "Übermittlung". Versuche, aus der organisationsrechtlichen Einheit der Gemeinde auch eine datenschutzrechtliche Einheit zu folgern, müssen hieran scheitern. Gleiches gilt für Ansätze, die um eines einheitlichen Stellenbegriffs willen die Übermittlungsregeln nur analog anzuwenden oder gar datenschutzrechtliche Schranken der Organisationskompetenz des jeweiligen Behördenleiters zu überlassen suchen.

Noch einmal: Jede Weitergabe eines personenbezogenen Datums zu einem anderen Zweck als demjenigen, der ursprünglich Grund für seine Speicherung und Verarbeitung war, ist eine "Übermittlung". Jede Offenbarung eines Datums gegenüber einer mit abweichenden Verwaltungsaufgaben betrauten Stelle zur Erfüllung eigener Zwecke stellt ebenfalls eine Übermittlung dar. Die zufällige organisatorische Zusammenfassung von Stellen mit unterschiedlichen Aufgaben kann nicht zu einem erheblich verminderten Datenschutz führen. Dies muß auch für die Gemeinde als ämterübergreifende Verwaltungseinheit gelten. Ihre datenschutzrechtliche Aufteilung in eine Vielzahl speichernder Stellen je nach deren Funktion ist eine unabdingbare Voraussetzung für einen wirksamen und umfassenden Datenschutz.

4.4
Praxis der Datenschutzkontrolle

4.4.1
Vorbemerkung

Die Kontrolltätigkeit der Dienststelle wurde auch im Jahre 1981 in verstärktem Maße fortgesetzt. Die große Anzahl "speichernder Stellen" im Geltungsbereich des HDSG und der mit der Vorbereitung und der Durchführung von Prüfungen verbundene zeitliche und personelle Aufwand haben im Hinblick auf die mir zur Verfügung stehenden personellen und sachlichen Mittel eine sorgfältige und gezielte Auswahl der zu prüfenden Objekte notwendig gemacht. Ausgewählt wurde u.a. nach der (geschätzten) Aussagekraft der zu erwartenden Prüfungsergebnisse im Hinblick auf deren "Multiplikationsfaktor", d.h. ihre Nachvollziehbarkeit durch andere Verwaltungen. Keine Rolle spielte, ob eine eigene DV-Anlage benutzt wurde oder die Datenverarbeitung als Auftrag an ein Rechenzentrum vergeben war.

Die Anzahl der 1981 durchgeführten Prüfungen im Verhältnis zur Zahl der speichernden Stellen - soweit diese durch die Meldung der von ihnen geführten Dateien zum Dateienregister bekannt sind - läßt keine umfassende Aussage aufgrund von statistisch auswertbaren Ergebnissen über den Stand der Datensicherungsmaßnahmen bei öffentlichen Stellen in Hessen zu. Trotzdem ist das Gesamtbild der inzwischen vorliegenden Erfahrungen so eindeutig - dies gilt auch im Hinblick auf die Prüfungsergebnisse der Vorjahre - daß eine zusammenfassende Aussage gemacht werden kann. Diese soll nicht zuletzt Anregung und Hinweis für diejenigen sein, die mit den Problemen des Datenschutzes und der Daten sicherung "vor Ort" befaßt sind.

4.4.2
Durchführung der Kontrollen

4.4.2.1
Ziel der Prüfungen

Ziel einer Prüfung ist im allgemeinen die Feststellung und Begutachtung aller Maßnahmen, die von der zu prüfenden Stelle getroffen wurden, um eine "sichere" Datenverarbeitung im Sinne des HDSG zu gewährleisten. Nicht die Datensicherung allein ist Prüfobjekt, sondern sämtliche Maßnahmen zur Erfüllung der Forderungen des

HDSG, etwa Auskunftserteilung, Berichtigung, Sperrung, Löschung, um nur einige zu nennen. Angestrebtes Ergebnis muß dabei stets die Wahrung der schutzwürdigen Belange der Betroffenen, darf also nicht lediglich die Berücksichtigung der administrativen Interessen der speichernden Stelle sein. Dies schließt auch eine Prüfung auf Vollständigkeit und Zweckmäßigkeit einzelner Maßnahmen ein.

Der mit der Vorbereitung und Durchführung solcher Prüfungen verbundene zeitliche und personelle Aufwand beruht im allgemeinen auf den komplexen Organisationsstrukturen, insbesondere der Unübersichtlichkeit des Aufgabenumfangs und der organisatorischen Abgrenzungen einzelner Verwaltungseinheiten zueinander, der Art und dem Umfang der zirkulierenden Daten, der zahlreichen anzuwendenden Rechtsvorschriften und der Vielfalt der eingesetzten technischen Mittel der Datenverarbeitung.

4.4.2.2
Vorbereitungen

Um einen effektiven Prüfungsablauf zu erreichen und nicht zuletzt auch die Behinderung des Geschäftsablaufs der zu prüfenden Stelle auf ein Mindestmaß zu reduzieren, sind umfangreiche Vorarbeiten zu leisten.

Die schriftliche Ankündigung der Prüfung und die Abstimmung des Termins erfolgen etwa zwei bis drei Wochen vorher, soweit es sich nicht um eine geringfügige "Anlaßprüfung" handelt. Mit der Ankündigung ergeht die Bitte, folgende Unterlagen vorzulegen:

- Organisationspläne
- ausgewählte Stellenbeschreibungen (z.B. für Angelegenheiten des Datenschutzes, DV-Personal)
- Organisationsverfügungen zur Regelung von Datenverarbeitung, Datensicherung und Datenschutz
- Konfigurationslisten (Art und Umfang der eingesetzten DV-Geräte)
- Netzpläne (Datenfernübertragung, -verarbeitung)
- Übersichten über die eingesetzten Programme (ausgenommen landeseinheitliche DV-Verfahren)
- Beschreibung eventuell zur Anwendung kommender Datensicherungsprogramme
- Vertragsunterlagen bei Auftragsdatenverarbeitung (§ 4 HDSG)
- Veröffentlichungen (§ 17 HDSG)

Bereits in der Vorbereitungsphase werden auch die im Dateienregister gespeicherten Meldungen der zu überprüfenden Stelle ausgewertet und stichprobenartig mit den Meldungen anderer Behörden gleicher Aufgabenzuweisung auf Inhalt und Umfang hin verglichen.

4.4.2.3
Ablauf der Prüfung

Eröffnet wird die Prüfung mit einem Gespräch bei dem jeweiligen Behördenleiter und dessen zuständigen Mitarbeitern sowie dem Beauftragten für Angelegenheiten des Datenschutzes. Im Rahmen dieses Gesprächs werden Aufgabenstellung, Prüfungsumfang und -dauer sowie die erbetene Unterstützung besprochen und die zeitliche Festlegung für Einzelprüfungen in verschiedenen Organisationseinheiten getroffen. Sinn dieser Einzelprüfungen ist es, einen Überblick über die Arbeitsweise einzelner Verwaltungsgliederungen und der bei ihnen zirkulierenden Daten zu erhalten. Dort vorhandene Dateien werden stichprobenartig auf ihren Datenumfang untersucht und mit den vorliegenden Auszügen aus dem Dateienregister verglichen; die Rechtsgrundlage der Verarbeitung wird geprüft und die dazugehörenden Akten werden, soweit vorhanden, mit einbezogen. Gespräche mit den Sachbearbeitern geben diesen Gelegenheit, die Probleme aus ihrer Sicht darzustellen.

Rahmen und Hilfsmittel einer Prüfung sind u.a. der Erlaß des Hessischen Ministers des Innern zur Durchführung des Hessischen Datenschutzgesetzes vom 2. Oktober 1978 (StAnz. 41/1978 S. 2011) und der Erlaß zur Durchführung des Bundesdatenschutzgesetzes (Datenschutz im nicht-öffentlichen Bereich; Neufassung der Vorläufigen Verwaltungsvorschriften zum Bundesdatenschutzgesetz vom 2. Februar 1981, StAnz. 4/1981 S. 425), der, soweit er Maßnahmen zur Datensicherung betrifft (Teil C, Abschnitt I III), sinngemäß Anwendung findet, sowie weitere bereichsspezifische Vorschriften. Technische Einrichtungen der Datenverarbeitung werden anhand eigener Checklisten auf die getroffenen Maßnahmen hin überprüft.

Die Einzelergebnisse, die innerhalb der Prüfung anfallen, werden, soweit es zur Klärung von Einzelheiten und Zusammenhängen erforderlich ist, mit den verantwortlichen Mitarbeitern der Verwaltung besprochen und in einem Protokoll festgehalten. Nach Abschluß der Gesamtprüfung erfolgt eine vorläufige Grobauswertung der Prüfungsergebnisse. Diese sind dann Gegenstand des Abschlußgesprächs mit der Behördenleitung.

4.4.2.4
Prüfungsbericht und Erfolgskontrolle

Die sich aus der Prüfung ergebenden Erfahrungswerte und Feststellungen werden in meiner Dienststelle ausgewertet, gewichtet und in einem schriftlichen Bericht festgehalten. Dieser geht der geprüften Stelle und deren Aufsichtsbehörde mit der Bitte um Stellungnahme zu. Er schildert im wesentlichen den Ablauf der Prüfung und zeigt Mängel - aber auch angetroffene positive Regelungen - auf. In Abstufung der Priorität der zu treffenden Maßnahmen wird im Bericht unterschieden zwischen

- der Beanstandung gem. § 26 HDSG;
- Mängeln, die unverzüglich zu beheben sind;
- Verfahrenslücken, die einer kurzfristigen Änderung bedürfen und
- Empfehlungen, die mittelfristig in die organisatorische Planung Eingang finden sollen.

Nach Ablauf einer angemessenen Frist - sie wird u.a. auch von dem gewonnenen Gesamteindruck bestimmt - erfolgt die schriftliche Aufforderung an die geprüfte Stelle, die von ihr gezogenen Konsequenzen darzulegen. Nachprüfungen erfolgen je nach Art des Einzelfalles.

4.4.3
Ausgewählte Beispiele

4.4.3.1
Erläuterungen

Die hier aufgeführten Beispiele befassen sich ausschließlich mit den Prüfungsergebnissen von **technischen** und **organisatorischen** Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung. Fragen der **Rechtmäßigkeit** der Datenverarbeitung sind in diesem Tätigkeitsbericht in den jeweiligen Sachabschnitten abgehandelt.

4.4.3.2
Hochschul- und Klinikrechenzentrum der Justus-Liebig-Universität Gießen

Die DV-Einrichtungen des Hochschul- und des Klinikrechenzentrums der Justus-Liebig-Universität in Gießen sind in einem gemeinsamen Funktionsbau untergebracht. Dieses Gebäude, einzig für diesen speziellen Zweck konzipiert, wurde 1980 endgültig in Betrieb genommen. Bereits im Jahre 1979 fand ein erstes Gespräch zwischen der Hochschule und dem Hessischen Datenschutzbeauftragten über geplante technische und organisatorische Maßnahmen im künftigen Rechenzentrum statt. Der Leiter des Hochschulrechenzentrums legte schon damals einen Antrag der Hochschule an den Hessischen Kultusminister (Sicherheitsmaßnahmen für den Rechnerraumbereich im Neubau des Hochschulrechenzentrums) vor. Diesem Antrag war zu entnehmen, daß das Hochschulbauamt die Kosten der geplanten Gebäudesicherungsmaßnahmen auf ca. 200000 DM geschätzt hat, im Vergleich zu den Gesamtkosten der Baumaßnahme von über 10 Millionen DM sicherlich keine unangemessene Summe. Im Hinblick auf die Kosten und "... weil im Bereich der Universität **nirgends** ein besonderer Objektschutz gegen Zerstörung eingerichtet ist", verzichtete das Hochschulbauamt auf die Durchführung dieser Gesamtmaßnahme und holte lediglich Angebote für Melde- und Überwachungseinrichtungen (Brand, Einbruch) in Höhe von ca. 35000 DM ein, eine bereits zu diesem Zeitpunkt zu kritisierende Entscheidung.

Zur gleichen Zeit begann das Institut für medizinische Statistik und Dokumentation der Universität Gießen mit dem Aufbau und der maschinellen Verarbeitung eines hessischen Krebsregisters. Das Echo, das diese hochsensitive Datensammlung in weiten Kreisen der Öffentlichkeit fand und ein mir zwischenzeitlich vorliegender Prüfungsbericht des Hessischen Rechnungshofs vom Sommer 1980, der u.a. ebenfalls auf die mangelnde Anlagensicherung hinwies, veranlaßten mich im Mai 1981, eine zweite Besichtigung des Funktionsgebäudes vorzunehmen, um mich über den Stand der Datensicherungsmaßnahmen zu unterrichten.

Das Ergebnis dieser Prüfung veranlaßte mich, eine formelle Beanstandung gem. § 26 HDSG auszusprechen. Die Rechenzentren der Hochschule und des Klinikums erfüllten nicht einmal den Mindeststandard an Sicherungsmaßnahmen, der von einem vergleichbaren Rechenzentrum des hessischen DV-Verbundes gefordert wird. Im Gegenteil, sie waren praktisch ungesichert. So war u.a. zu beanstanden, daß die mit Normalglas versehenen Zugangstüren lediglich über handelsübliche Sicherheitsschlösser verfügten; die Außenfenster - mit Normalglas ausgestattet -waren ungesichert. Zwar war eine Feuermeldeanlage installiert, aber kein zur Polizei geschalteter Einbruchmelder. Alle Funktionsräume waren im wesentlichen von außen voll einsehbar; das gesamte Rechenzentrumsgebäude blieb ab 22 Uhr unbewacht. Besonders bedauerlich ist, daß bereits bei der Bauplanung versäumt wurde, die

ursprünglich vorgesehenen Gebäudesicherungsmaßnahmen durchzusetzen. Inzwischen steht fest - was die von dem Hochschulbauamt aufgrund meiner Beanstandung wiederaufgenommenen Planungen bestätigen - ,daß eine nachträgliche Durchführung von Gebäudesicherungsmaßnahmen in dem erforderlichen Umfang über die früheren Kostenschätzungen hinausgehen dürfte. Ganz zu schweigen von den Problemen, die bei der Verwirklichung der Maßnahmen für den technischen Betrieb innerhalb des Rechenzentrums entstehen können.

4.4.3.3
Neubau eines Rechenzentrums für die Fachhochschule Frankfurt am Main

In Frankfurt am Main wird derzeit ein neues Verfügungsgebäude für die Fachhochschule errichtet. Dieses Gebäude soll im Erdgeschoß und im ersten Stock das Rechenzentrum und Datenträgerräume aufnehmen. Im Januar 1981 fand in Frankfurt eine gemeinsame Bauplanbesprechung mit der Hochschule, dem Hochschulbauamt, dem Bauträger, der Polizei Frankfurt und mir statt. Ziel dieser Beratungen war es, im zukünftigen Rechenzentrumsbereich wirksame Sicherungsmaßnahmen einzuplanen. Die Vertreter der Hochschule standen den vorgeschlagenen Maßnahmen eher skeptisch gegenüber und zweifelten teilweise deren Verhältnismäßigkeit im Sinne des § 10 HDSG an. Es zeigte sich aber, daß in gemeinsamer Beratung nicht nur zahlreiche neue Anregungen gefunden, sondern auch in der Rohbauphase des Gebäudes noch ohne größeren Aufwand eingeplant werden konnten.

Das Hochschulrechenzentrum hat inzwischen in einem Schreiben an das Hochschulbauamt die Realisierung einer Reihe von Vorkehrungen angekündigt. Werden die Maßnahmen wie vorgesehen durchgeführt, halte ich die Datensicherung des Hochschulrechenzentrums aus bautechnischer Sicht für ausreichend.

4.4.3.4
Gesamthochschule Kassel (Funktionsbau)

Um die Erfahrungen zu vervollständigen, die sich aus den Prüfungen in Frankfurt und Gießen ergeben hatten, besuchten Mitarbeiter meiner Dienststelle im Anschluß daran die Gesamthochschule Kassel und fanden dort eine ähnliche Situation wie in Gießen vor.

Das Ergebnis der Begehung des neu errichteten Funktionsgebäudes und der Gespräche mit dem Leiter und Mitarbeitern des Rechenzentrums läßt sich in einem Satz zusammenfassen: Maßnahmen zur Gebäude- und Anlagensicherung waren nicht durchgeführt worden. Immerhin hatte sich der Leiter des Rechenzentrums mit Erfolg bemüht, zumindestens solche organisatorischen Maßnahmen zur Gewährleistung eines Minimums von Datenschutz und Datensicherung zu treffen, die er ohne finanzielle Mittel verwirklichen konnte.

Die Folge der Versäumnisse bei der Planung des Neubaus sind auch in diesem Fall zumindest eine längere Phase der Unsicherheit der Datenverarbeitung, eine aufwendige nachträgliche Ausstattung des Gebäudes sowie größere Behinderungen für die Datenverarbeitung während des Umbaus.

4.4.3.5
Archivierung von Patientenakten der Universität Marburg

Anläßlich einer "Hausbesetzung" durch Studenten der Universität Marburg im Dezember 1980 - sie fand große Aufmerksamkeit in Rundfunk und Presse - informierten mich die Hochschule und Vertreter des ASTA darüber, daß in dem besetzten Gebäude, dem leerstehenden alten Marburger Stadtgefängnis, große Mengen Patientenakten der Universitätskliniken unsachgemäß und ungesichert lagerten. Eine sofort durchgeführte Ortsbesichtigung ergab: Die Patientenunterlagen wurden in Zellen und ehemaligen Gemeinschaftsräumen aufbewahrt. Diese Räume sind nach außen vergittert, nach innen waren sie teilweise unverschlossen, teilweise mit Sicherheitsschlössern versehen.

Die festgestellten Sicherungsmaßnahmen - es wurden ausnahmslos ladenneue Ketten und Schlösser, auf denen noch die Preisschilder klebten, vorgefunden - ließen darauf schließen, daß die Zugangssicherungen vor der "Hausbesetzung" nicht ausreichend waren. Eine Zugangsregelung für das Archiv im Gefängnis existierte nicht. Unter den gegebenen Verhältnissen war der Zugang auch kaum kontrollierbar. Die Universität hat dargelegt, daß ihr die Unzulänglichkeit der Archivsicherung bekannt ist, sie sich aber nicht in der Lage sieht, dies kurzfristig zu ändern. Unter Hinweis auf die Schutzbedürftigkeit der Daten in den dort lagernden Akten, die der ärztlichen Schweigepflicht unterliegen, habe ich angeregt, daß die Universität entsprechende Zugangsregelungen erläßt und künftig eine ständige Kontrolle der Sicherungsmaßnahmen stattfindet.

4.4.3.6
Allgemeine Ortskrankenkasse in Wiesbaden

Diese Prüfung sollte dazu dienen, einen Eindruck von der Verwirklichung des Datenschutzes bei einer großen Ortskrankenkasse zu gewinnen und beschränkte sich auf einige Schwerpunkte. Entscheidend für die Auswahl der AOK Wiesbaden war u.a. die Tatsache, daß diese über ein größeres, eigenes Rechenzentrum verfügt. Der Prüfungsbericht enthält Empfehlungen und kritische Anmerkungen zur Verbesserung des Datenschutzes, die jedoch durchweg nicht auf akuten Fällen der Gefährdung des Datenschutzes beruhten; er hatte vielmehr die Aufgabe, auf mögliche Schwachstellen aufmerksam zu machen. Als Ergebnis wurden folgende Empfehlungen ausgesprochen:

- In Fällen der Auftragsdatenverarbeitung für die AOK durch externe Firmen sollten künftig diese Auftragnehmer auf die von ihnen getroffenen Maßnahmen zur Gewährleistung der Datensicherung geprüft werden. Dazu gehört auch die Frage der Löschung der dort verarbeiteten Daten.
- Die bestehenden Organisationsregelungen für die Großraumbüros der AOK sind auf Maßnahmen der Datensicherung (Aufbewahrung von Akten und Mikrofiches, Zugangsregelungen - auch für Mitarbeiter -, Vertraulichkeit des gesprochenen Wortes bei Kundenberatungen usw.) zu überprüfen.
- Erforderliche Funktionstrennungen zwischen Fachabteilungen und Datenverarbeitung sollten klarer beschrieben und vollzogen werden.
- Der Datenträgertransport ist auch für den Bereich der Fahr- und Botendienste schriftlich zu regeln.
- Gebäudesicherungsmaßnahmen im Bereich des Rechenzentrums sind an bestimmten Schwachstellen zu verbessern bzw. durchzuführen.
- Regelungen für den Katastrophenfall sind auch auf den Bereich des Rechenzentrums auszudehnen und dort auszuhängen.
- Es sind klare Regelungen für Verfahrensentwicklung und Verfahrensdurchführung zu erlassen.
- Der Bestand an Datenträgern ist beschleunigt auf das bereits vorhandene maschinelle Datenträgerverwaltungssystem zu überführen. Datenträger sollten dann nur noch mit numerischen Etiketten versehen werden. Regelmäßige Bestandsaufnahmen sind erforderlich. Die Anschaffung eines Bandreinigungs- und -löschgeräts sollte geprüft werden.

Die Geschäftsleitung der AOK Wiesbaden hat mir inzwischen mitgeteilt, daß aufgrund meiner Prüfungsempfehlungen nachstehende Maßnahmen realisiert wurden bzw. geplant sind:

- Die zur Auftragsdatenverarbeitung bestehenden Verträge werden auf die Einhaltung der Datenschutzbestimmungen hin überprüft und ggf. angepaßt.
- Eine unangemeldete Prüfung eines Auftragnehmers wurde durchgeführt.
- In den Großraumbüros ist durch organisatorische Maßnahmen sichergestellt, daß alle Unterlagen mit personenbezogenen Daten nach Dienstschluß wegzuschließen sind. Kontrollen werden durch den Hausmeister bzw. den Pförtner nach Dienstschluß durchgeführt.
- Im Rechenzentrum wurde eine Funktionstrennung zwischen Produktion und Programmierung hergestellt. Die Programmierer und der Leiter des Rechenzentrums haben ihre Arbeitsplätze in neuen Räumen getrennt von den Produktionseinrichtungen. Die Kontakte zwischen Fachabteilung und dem Rechenzentrum wurden durch Verwaltungsanordnung im einzelnen festgelegt. Arbeitsaufträge werden nur noch von der Annahmestelle des Rechenzentrums angenommen.
- Zur Erhöhung der Gebäudesicherung ist für den Maschinenraum des Rechenzentrums einschließlich des Archivs der Einbau einer Einbruchmeldeanlage vorgesehen. Ein Katastrophenplan für das Rechenzentrum wurde inzwischen ausgehängt.
- Das Bandarchiv wird beschleunigt auf maschinelle Datenträgerverwaltung umgestellt. Ein Bandreinigungs- und -löschgerät mit Kennsatzschutz ist inzwischen beschafft worden.
- Der Leiter des Rechenzentrums wurde verpflichtet, auch die übrigen Prüfungsempfehlungen entsprechend umzusetzen.

4.4.3.7
Landkreisverwaltung Waldeck-Frankenberg

Der Prüfungsbesuch beim Landrat des Landkreises Waldeck-Frankenberg in Korbach verfolgte den Zweck, Erkenntnisse über die Verarbeitungsbedingungen im kommunalen wie staatlichen Bereich einer Kreisverwaltung zu gewinnen. Wegen der nur beschränkt verfügbaren Zeit konzentrierte er sich auf einzelne ausgewählte Organisationseinheiten des Kreises. Dazu gehörten: die zentrale Datenerfassungsstelle, das Archiv des Kreishauses, das Staatliche Schulamt, die Kfz-Zulassungsstelle mit dem Sachgebiet Fahrerlaubnisse, die Ausländerbehörde, das Sachgebiet Waffenwesen, die örtliche Dienststelle der Kriminalpolizei, das Personalamt und das Kreisjugendamt.

Im einzelnen gibt der Prüfungsbericht folgende Empfehlungen:

- Eine Bestandsaufnahme der bisher getroffenen Datensicherungsmaßnahmen ist vorzunehmen. Die festgestellten Regelungsdefizite sind durch schriftliche Organisationsverfügungen zu beheben und die entsprechenden technischen Maßnahmen zur Gewährleistung der Datensicherung und Gebäudesicherung zu ergreifen. Dabei ist der Erlaß des Hessischen Ministers des Innern zur Durchführung des Bundesdatenschutzgesetzes (StAnz. 7/1981 S. 425) sinngemäß anzuwenden.

- Die Auftragsdatenverarbeitung der kreisangehörigen Gemeinden, der Kreisverwaltung und der Stadt Korbach untereinander bedarf einer erweiterten vertraglichen Regelung. In dieser Zusatzvereinbarung sind insbesondere Art und Umfang der Datenverarbeitung zu beschreiben. Die Prüfungskompetenzen der Beauftragten für den Datenschutz sind festzulegen; zu regeln sind die Behandlung und der Verbleib von Maschinenprotokollen.

- Die Archivierung von Daten und Datenträgern (auch Akten) bedarf einer generellen Regelung (z.B. über Zugang, Abgang, Übergabe an Archive). Sobald die räumlichen Voraussetzungen gegeben sind, ist eine Trennung des Archivs nach Organisationseinheiten vorzunehmen.

- Das Problem der Vernichtung von Daten und Datenträgern (auch Akten) ist für die gesamte Kreisverwaltung zu lösen. Die Beschaffung eines bzw. mehrerer mechanischer Aktenvernichter ist empfehlenswert.

- Es ist zu prüfen, ob tatsächlich alle gesetzlich vorgesehenen Dateien zum Dateienregister des Hessischen Datenschutzbeauftragten gemeldet wurden bzw. ob nicht Dateien irrtümlicherweise als "intern" eingestuft wurden, obwohl aus ihnen Daten übermittelt werden.

Fehlende Zugangs- und Sicherungsvorkehrungen bilden auch im übrigen die Grundlage für den Hauptteil der ausgesprochenen Empfehlungen. Soweit Bedenken an der Rechtmäßigkeit einzelner Maßnahmen der Datenverarbeitung entstanden, wurden diese im einzelnen erläutert.

4.4.4
Häufigste Regelungsdefizite

Die Auswertung aller vorliegenden Prüfungserfahrungen ließ im Bereich der maschinellen und der manuellen Datenverarbeitung am häufigsten folgende Mängel und Regelungsdefizite erkennen:

- Vorhandene Dateien wurden zwar von den geprüften Stellen in der Regel erfaßt; der "Ist-Zustand" der manuellen und maschinellen Datenverarbeitung wird jedoch nur ansatzweise ermittelt.

- Gesamtpläne zur Regelung technischer und organisatorischer Fragen der Datensicherung und des Datenschutzes waren nirgends vorhanden. Soweit Einzelregelungen vorlagen, beruhten diese oft auf mündlichen Absprachen und waren nicht nachkontrollierbar; schriftliche Regelungen - auch in Stellenbeschreibungen - fehlten fast immer.

- Im Bereich der Organisation fehlten durchgängig klare Regelungen. Funktionstrennungen wurden nicht eingehalten, Dokumentationen und andere Arbeitsmittel (Handbücher, Richtlinien, Katastrophenpläne) waren unvollständig oder nicht aktualisiert.

- Im Bereich der Zugangskontrollen fehlten Protokollierungen; Regelungen für die kurzzeitige Abwesenheit vom Arbeitsplatz waren nicht vorhanden. Regelungen für den Besucherverkehr fehlten.

- Bei der maschinellen Datenverarbeitung fiel die mangelnde Trennung in Funktionsbereiche auf; closedshop-Betrieb (soweit überhaupt vorhanden) wurde oft nur unvollständig durchgeführt.

- Zugangsregelungen außerhalb der Dienstzeit (z.B. an Sonn- und Feiertagen) waren vielfach lückenhaft.

- Erhebliche Mängel wurden in der technischen Sicherung von Gebäuden, Räumen und Anlagen festgestellt.

- Die Datenträgerverwaltung, die Aufbewahrung von Erfassungsbelegen, Dateien und dazugehörenden Unterlagen wiesen gravierende Mängel auf.
- Eine Verbleibskontrolle entnommener Datenträger, Karteikarten, Akten oder sonstiger Unterlagen war in vielen Fällen nicht möglich.
- Geregelte Verfahren zur Vernichtung bzw. Löschung nicht mehr benötigter Datenträger fehlten.
- Bei der Datenfernverarbeitung wurden in den Betriebssystemen vorhandene Möglichkeiten der Datensicherung nicht oder unzureichend wahrgenommen. So war die Verwendung von Paßwörtern nicht generell vorgeschrieben. Konsolprotokolle wurden nur unregelmäßig oder überhaupt nicht ausgewertet.
- Zwar wurden fast immer die sog. log- und accounting-Aufzeichnungen zur Prüfung des Systemverhaltens ausgewertet, nicht aber die Systemaktivitäten der Benutzer der DV.
- Auftragsdatenverarbeitung wurde auf der Grundlage unzureichend geregelter Auftragsverhältnisse praktiziert.
- Kontrollen der auftraggebenden Stellen beim Auftragnehmer waren fast nie erfolgt. Es bestanden somit auch keine Kenntnisse, ob und inwieweit der Auftragnehmer geeignete Vorkehrungen zur Gewährleistung des Datenschutzes und der Datensicherung getroffen hatte.
- Beim Transport von Datenträgern waren die verschiedensten Versandformen anzutreffen (Versand als Normalbrief, eigene oder externe Botendienste, Benutzung der Bundesbahn), ohne daß eindeutige Vorschriften über die zu wählende Versandart existieren.
- Für Botendienste fehlten eindeutige Vorgaben für die Auftragsstellung und Auftragsdurchführung. Dies führte immer wieder dazu, daß Datenträger oder Verarbeitungsergebnisse aus der Datenverarbeitung nicht den eigentlichen Adressaten erreichten, sondern bei anderen Dienststellen als "Irrläufer" kursierten. Auch meine Dienststelle erhielt auf diese Weise Magnetbänder und Auswertungen anderer öffentlicher Stellen.
- Bei den Fachabteilungen ist häufig gegenüber den DV-Abteilungen ein geringeres Bewußtsein für Probleme des Datenschutzes anzutreffen. Notwendige Vorkehrungen werden vielfach als "unverhältnismäßig" bezeichnet, ohne daß ausreichend bekannt ist, daß bisher schon der Umgang mit sensitiven personenbezogenen Daten den restriktiven Regelungen des Dienstrechts, des Steuergeheimnisses, des Statistikgeheimnisses oder anderer bereichspezifischer Vorschriften unterlag.

Freilich: So sehr die aufgezeigten Mängel zur Kritik Anlaß geben, so falsch wäre es, generell von einem unzureichenden Stand der technischen und organisatorischen Maßnahmen nach § 10 HDSG zu sprechen. Die hier aufgezeigten Beispiele sollen zum Nachdenken anregen und nochmals verdeutlichen, daß der Datenschutz organisatorische Konsequenzen hat. Die Einführung neuer Techniken erfordert auch eine Überprüfung bestehender Strukturen und Organisationsformen, eine Neuformulierung von Dienstanweisungen und die Kontrolle auf Einhaltung der entsprechenden Vorschriften. Auf keinen Fall dürfen aber - wie in der Vergangenheit immer wieder geschehen - alle mit Kosten verbundenen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherung als "unverhältnismäßig" im Sinne des § 10 HDSG verworfen werden. Dies führt allenfalls dazu, daß - wie im Hochschulbereich - später aufgrund von Beanstandungen umfangreiche und teure Umbauarbeiten notwendig sind, die bei rechtzeitiger Realisierung nur einen Bruchteil der letztlich entstehenden Kosten verursacht hätten.

4.5
Exemplarische Einzelfälle

Die folgenden Fälle sind nur ein kleiner Ausschnitt der Einzelprobleme, mit denen ich im Berichtszeitraum befaßt war. Sie sind unter zwei Gesichtspunkten ausgewählt: Zum einen danach, ob sich aus ihnen wichtige neue datenschutzrechtliche Problemaspekte ergeben, zum anderen danach, ob Konsequenzen für die Verwaltungstätigkeit besonders dringlich erscheinen.

4.5.1
Masseneinwendungen im atomrechtlichen Genehmigungsverfahren

Die Genehmigungsverfahren bei industriellen Großvorhaben stellen die betroffenen Behörden in verstärktem Maße vor das Problem, eine Vielzahl von Einwendungen bearbeiten zu müssen. So hatten im atomrechtlichen Genehmigungsverfahren zum Block C des Kernkraftwerks Biblis ca. 26000 Personen Einwendungen auf Sammeleinspruchsformularen erhoben, etwa weitere 100 brachten Einwendungen in individuellen Schreiben vor. Name

und Anschrift der Einwender, das Datum der jeweiligen Einwendung und ihre Form (Sammel- oder Einzeleinspruch) waren zu erfassen, um für verfahrensrechtliche Entscheidungen wie die Überprüfung des Zutrittsrechts zum nichtöffentlichen Erörterungstermin, die Reihenfolge der Behandlung der Einwendungen und die Feststellung der Klagebefugnis im eventuellen späteren Verwaltungsstreitverfahren zur Verfügung zu stehen. Soweit diese Daten im Auftrag des Hessischen Ministers für Wirtschaft und Technik beim Hessischen Statistischen Landesamt auf Lochkarten übertragen wurden und von der Hessischen Zentrale für Datenverarbeitung zu Einwenderlisten verarbeitet wurden, bestanden keine datenschutzrechtlichen Bedenken. Nach der Erstellung der Listen wurden die dafür benutzten Magnetbänder gelöscht und die Lochkarten vernichtet.

Einer der betroffenen Einwender wandte sich an mich und bat um eine Überprüfung der datenschutzrechtlichen Zulässigkeit der Kontrollmaßnahmen vor der nichtöffentlichen Anhörung. Der Minister hatte ein privates Überwachungsunternehmen mit der Zutritts- und Personenüberprüfung beauftragt und diesem dazu die Listen der Einwender ausgehändigt.Die darin liegende Datenübermittlung war zulässig,da die Beauftragung der Privatfirma zur Wahrnehmung der Kontrollbefugnisse der Genehmigungsbehörde erforderlich war. Wie der Wirtschaftsminister erklärte, hätte die angespannte Personalsituation eine Überprüfung durch Mitarbeiter seines Hauses nicht zugelassen. Durch entsprechende Belehrung des Überwachungspersonals, das Einsammeln der Listen nach Abschluß der täglichen Erörterung sowie die ständige Beaufsichtigung der die Eingangskontrolle durchführenden Bediensteten durch Mitarbeiter des Ministers wurde darüberhinaus dafür Sorge getragen, daß die Überwachungsfirma ihrer Verpflichtung gerecht wurde, die übermittelten Daten nicht zu anderen Zwecken zu verwenden.

4.5.2
Kontrollmitteilungen an die Finanzämter

Eine Vielzahl von Behörden, aber auch private Stellen mit öffentlichen Zuschüssen übersenden den Finanzämtern regelmäßig sog. "Kontrollmitteilungen" über Honorare, Vergütungen, Gebühren oder Zuschüsse, die von ihnen an Privatpersonen ausgezahlt worden sind. Diese Meldungen dienen der Überprüfung der Steuererklärungen der Empfänger. In einer Eingabe wurde ich z.B. mit der Aufforderung des Hessischen Rechnungshofs an das Landesversorgungsamt Hessen befaßt, die an Ärzte gezahlten Gebühren für sog. Befundberichte oder "Hausarztmitteilungen" ab einem jährlichen Gesamtbetrag von 300 DM der jeweils zuständigen Steuerbehörde mitzuteilen. Der Hessische Finanzminister hat mit Erlaß vom 3. August 1970 (StAnz. S. 1654) generell die Übermittlung von Kontrollmitteilungen angeordnet.

Niemand zweifelt daran, daß es ein legitimes Ziel der Steuerverwaltung ist, die ordnungsgemäße Versteuerung öffentlicher Mittel durch den Empfänger zu überwachen. Der Bürger kann jedoch auch zu Recht fordern, daß entsprechende Mitteilungen an sein Finanzamt nur dann ergehen, wenn dies für ihn ersichtlich aufgrund eines förmlichen Gesetzes oder einer auf einem Gesetz beruhenden Vorschrift geschieht.

Rechtsgrundlage für die Einholung von Auskünften durch die Steuerbehörden sind die §§ 93 f., 111 ff. Abgabenordnung (AO). Nach § 111 Abs. 1 AO haben u.a. alle Behörden die zur Durchführung der Besteuerung erforderliche Amtshilfe zu leisten. "Amtshilfe" bedeutet jedoch "Hilfe im Einzelfall". Amtshilfe darf nicht auf Dauer angelegt sein, etwa derart, daß die ersuchte Behörde ständig bestimmte Dienstgeschäfte für die auftraggebende Stelle durchführt. Ich habe Bedenken, ob lediglich aufgrund eines Erlasses des Finanzministers (s.o.) in einer Vielzahl von gleichgelagerten Fällen ohne zeitliche und örtliche Begrenzung die Anweisung zur regelmäßigen Datenübermittlung gegeben werden darf. Zusätzliche Zweifel ergeben sich daraus, daß dieser Erlaß als Vollzugsmaßnahme zu § 64a der Reichshaushaltsordnung konzipiert war, einer Norm, die keine Auswirkung gegenüber dem Bürger hatte, sondern lediglich die ordnungsgemäße und sparsame Wirtschaftsführung der Verwaltung zum Gegenstand hatte. Die Übermittlung personenbezogener Daten bedarf als grundrechtsrelevanter Eingriff hingegen einer Ermächtigungsnorm im Verhältnis zum betroffenen Bürger. Der Erlaß als solcher erfüllt aufgrund seiner mangelnden Qualität als Rechtsnorm diese Voraussetzungen nicht. § 64 a RHO ist auch aufgrund der Bundeshaushaltsordnung vom 19. August 1969 zum 1. Januar 1970 außer Kraft getreten (§ 119 BHO). Die an seine Stelle getretenen, jetzt geltenden Bestimmungen, etwa §§ 23, 44 BHO enthalten ebenfalls keine Ermächtigung für eine derartige Praxis.

Auch die Abgabenordnung selbst beinhaltet Schranken, die ihr entgegenstehen. Die Auskunftspflicht der Beteiligten und anderer Personen im allgemeinen Festsetzungsverfahren nach § 93 AO ist durch den "Subsidiaritätsgrundsatz" in § 93 Abs. 1 S. 3 AO gekennzeichnet. Danach ist prinzipiell zuerst der Steuerpflichtige zur Auskunftserteilung heranzuziehen. Dritte sollen nur befragt werden, "wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt und keinen Erfolg verspricht." Diese Vorschrift regelt zwar nicht unmittelbar die Auskunftserteilung durch dritte Behörden. Aus § 111 Abs. 1 S. 1 AO ergibt sich jedoch, daß nur die **erforderliche** Amtshilfe zu leisten ist. Das heißt auch, daß dem Rechtsgedanken des § 93 Abs. 1 S. 3 AO Rechnung zu tragen ist und nur im Falle der Erfolglosigkeit oder Aussichtslosigkeit der Nachfrage beim Bürger eine andere Behörde um die Übermittlung steuerlich relevanter Hinweise gebeten werden kann.

Sowohl der Begriff der auf den Einzelfall zu beschränkenden Amtshilfe als auch dieser in §§ 111 Abs. 1 i.V.m. 93 Abs. 1 S. 3 AO verankerte Grundsatz stehen somit einer regelmäßigen Übermittlung von Kontrollmitteilungen an die Finanzämter entgegen.

Ich habe den Finanzminister um eine Übersicht über die derzeit praktizierten Verfahren der Kontrollmitteilungen gebeten; sie liegt mir zur Zeit noch nicht vor. Meinen Hinweis auf die Rechtslage beantwortete der Minister damit, daß dieses Problem zwischen dem Bundesminister der Finanzen und der Ständigen Konferenz der Datenschutzbeauftragten der Länder und des Bundes erörtert werden solle. Ein solches Gespräch ist jedoch bisher nicht zustandegekommen. Da zu erwarten ist, daß sich zum einen eine bundesweite Lösung des Problems nicht vor Ablauf einer längeren Frist abzeichnen wird, zum anderen aber das System der "Kontrollmitteilungen" eine große Anzahl von Bürgern betrifft, sollte diese Frage von der Hessischen Landesregierung aufgegriffen werden.

4.5.3
Übermittlung der Daten von Krankenhauspatienten an die Polizei

Im Zusammenhang mit der ärztlichen Behandlung von verletzten Demonstranten erhielt ich die Anfrage, inwieweit das Personal eines Krankenhauses gegenüber der Polizei zur Bekanntgabe der personenbezogenen Daten von Patienten berechtigt bzw. verpflichtet ist.

Einem Auskunftsbegehren von Staatsanwaltschaft und Polizei im Zuge der Strafverfolgung (vgl. §§ 161, 161 a, 163 Strafprozeßordnung) steht zunächst grundsätzlich die ärztliche Schweigepflicht (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch) entgegen. Sie gilt auch für das ärztliche Hilfspersonal, wozu weitgehend auch die Verwaltungsbediensteten von Krankenhäusern gerechnet werden können (§ 203 Abs. 3 StGB). Im Strafverfahren findet diese Geheimhaltungspflicht ihren Ausdruck im Zeugnisverweigerungsrecht sowohl für Ärzte (§ 53 Abs. 1 Nr. 3 StPO) als auch für ärztliches Hilfspersonal (§ 53 a Abs. 1 StPO). Auch eine Beschlagnahme von Krankenakten bzw. der entsprechenden Kartei ist prinzipiell unzulässig, da das Gesetz ausdrücklich die Beschlagnahme solcher Gegenstände verbietet, auf die sich das ärztliche Zeugnisverweigerungsrecht erstreckt (§ 97 Abs. 1 Nrn. 2 und 3 StPO).

Eine Übermittlung persönlicher Angaben der Krankenhauspatienten - hier also der eingelieferten Demonstranten - ist nur ausnahmsweise zulässig, wenn einer der Rechtfertigungsgründe des Strafrechts für die Durchbrechung des ärztlichen Berufsgeheimnisses vorliegt. Da von einer stillschweigenden oder mutmaßlichen Einwilligung der Betroffenen sicher nicht ausgegangen werden kann, kommt hier im wesentlichen nur der sog. "rechtfertigende Notstand" (§ 34 StGB) in Betracht. Er setzt voraus, daß die Datenübermittlung zur Abwehr einer ernstlichen Gefahr für Rechtsgüter wie Leib, Leben, persönliche Freiheit o.ä. erfolgt und eine Abwägung ergibt, daß das Interesse an der Kenntnis der Daten das Interesse an ihrer Geheimhaltung wesentlich überwiegt. Beide Voraussetzungen gleichzeitig werden in den hier fraglichen Fällen nur selten gegeben sein.

Unbenommen bleibt der Polizei die Einsichtnahme in das Verzeichnis, das jedes Krankenhaus nach § 10 Hessisches Meldegesetz über die stationär aufgenommenen Patienten zu führen hat. In dieses Verzeichnis werden jedoch keine medizinischen Daten - wie etwa die Art der Verletzung oder die ärztliche Diagnose - aufgenommen, die wiederum Rückschlüsse über den Anlaß des Krankenhausaufenthalts ermöglichen könnten.

4.5.4
Amtshilfe im Ermittlungsverfahren und Schutz des Betroffenen

Das Landeskriminalamt (LKA) eines anderen Bundeslandes hatte sich im Rahmen eines Ermittlungsverfahrens wegen Verdachts der geheimdienstlichen Tätigkeit mit der Bitte um Amtshilfe an den Hessischen Kultusminister gewandt. Zur Überprüfung der Angabe des Betroffenen, er habe zu einem bestimmten Zeitpunkt an einer von ihm genannten Fachhochschule der DDR die Abschlußprüfung als Bibliothekar abgelegt, bat das LKA den Kultusminister, Personen ausfindig zu machen, die diese Angabe bestätigen könnten. Der Kultusminister richtete daraufhin einen entsprechenden Erlaß an alle Hochschulen und alle wissenschaftlichen Bibliotheken in Hessen.

Das Datenschutzproblem lag hier darin, daß in dem Erlaß allen 39 im Verteiler genannten Stellen ausdrücklich der Anfragegrund (Verdacht geheimdienstlicher Tätigkeit) und die anfragende Stelle (LKA...) mitgeteilt wurden. Für die Beschaffung der erbetenen Information durch den Kultusminister war die Bekanntgabe dieser Daten jedoch völlig unnötig. Ihre Weitergabe widerspricht dem "Erforderlichkeitsgrundsatz"für die Datenübermittlung (vgl. § 12 HDSG) und dem Grundsatz der Verhältnismäßigkeit des Eingriffs in die Privatsphäre. In Betracht kam auch ein Verstoß gegen die Geheimhaltungspflicht von Amtsträgern nach § 203 Abs. 2 StGB. Der schwerwiegende Eingriff in das Persönlichkeitsrecht des Betroffenen wird vor allem aus folgender Überlegung deutlich: Selbst wenn das Ermittlungsverfahren später eingestellt wird oder in einem Gerichtsverfahren ein Freispruch ergeht, wird er dennoch bei allen Adressaten des Erlasses irreparabel in seinem Ruf geschädigt bleiben.

Auf meine Beanstandung hin gab der Kultusminister - wenn auch erst nach zweimaliger Mahnung - eine ausführliche Stellungnahme ab. Sie enthält im einzelnen die Maßnahmen, die er zur Unterrichtung seiner Bediensteten und zur Handhabung vergleichbarer Amtshilfeersuchen in der Zukunft getroffen hat, um die Anforderungen des Datenschutzes einzuhalten. Dieser Einzelfall ist damit abgeschlossen. Seine Aufnahme in

diesen Bericht verstehe ich jedoch als Aufforderung an alle öffentlichen Stellen, bei der Abwicklung bzw. Weitergabe von Informationsersuchen der Sicherheitsbehörden in Ermittlungsverfahren so vorzugehen, daß der Schutz des Persönlichkeitsrechts der Betroffenen, insbesondere die Wahrung der Unschuldsvermutung nicht verurteilter Bürger, so weit wie möglich gewährleistet wird.

4.5.5
Regelmäßige Auswertung von Meldescheinen durch die Polizei

Die örtlichen Polizeidienststellen in Hessen streben - im Berichtsjahr verstärkt durch eine von ihnen gemeinsam beschlossene Aktion - eine möglichst lückenlose Kontrolle aller Wohnungsveränderungen der in ihren kriminalpolizeilichen personenbezogenen Sammlungen erfaßten Personen an. Ziel dieser Aktion ist es, Namen und Anschriften dieses Personenkreises auf aktuellem Stand zu halten, aber auch gesuchte Personen aufgreifen zu können. Zu diesem Zweck erging an die Gemeinden die Aufforderung, den Polizeidienststellen regelmäßig Durchschläge aller von den Bürgern anläßlich von Umzügen ausgefüllten Meldeformulare vorzulegen. Die gleiche Bitte um kurzfristige Überlassung zur Einsicht wurde an die Landratsämter gerichtet, da diese die Durchschläge von den kreisangehörigen Gemeinden erhalten, um diese an das Statistische Landesamt weiterzuleiten. Auf diese Weise erhält die Kriminalpolizei eine vollständige Übersicht über alle Meldevorgänge. Zudem bekommt sie Kenntnis nicht nur von Namen und Anschrift der betroffenen Bürger, sondern von allen auf dem Meldeschein eingetragenen Daten einschließlich der Religionszugehörigkeit und der Angaben über Mitbewohner.

Die Übermittlung der Daten **aller** umziehenden Bürger und des **gesamten** Meldedatensatzes ist für die Aufgabenerfüllung der Polizei nicht erforderlich und deshalb nach § 12 Abs. 1 HDSG rechtlich nicht zulässig.

Sie erhält nämlich erheblich mehr Daten, als sie benötigt: Vergleicht man die Zahlen der in kriminalpolizeilichen Sammlungen oder Suchdateien erfaßten Personen mit der Zahl der meldepflichtigen Bürger, so stehen beide Zahlen in keinem Verhältnis zueinander. Nur ein Bruchteil der Personalien wird tatsächlich gebraucht. Darüberhinaus enthalten auch die "verwertbaren" Scheine eine Menge überschüssiger Angaben. Hinzu kommt, daß die Polizei nach § 16 a Abs. 6 Hessisches Meldegesetz zur Erfüllung ihrer Aufgaben jederzeit Einsicht in das Melderegister nehmen kann; auf die regelmäßige Übermittlung aller Meldescheine ist sie daher nicht angewiesen.

Zweifel an der Anwendbarkeit von § 12 HDSG mit dem Hinweis auf den Begriff der "Datei" sind nicht angebracht: Zum einen stammen die Daten "aus dem Melderegister" als einer Datei. Würde man die Sammlung der Meldescheine im Verhältnis zum Melderegister als selbstständige Vorstufe ansehen, die nicht die Merkmale einer Datei erfüllt, so könnten auf diesem Weg der "Übermittlung aus den Meldescheinen" die Übermittlungsvorschriften über das Melderegister umgangen werden. Dies stünde jedoch im Widerspruch zum Gesetzeszweck. Vor allem aber stellt auch die Sammlung der Meldescheine eine Datei i.S.d. § 2 Abs. 3 Nr. 3 Hessisches Datenschutzgesetz dar, da die Formulare eine Vielzahl von Merkmalen erfassen und auch entsprechend umgeordnet und ausgewertet werden können.

Die geschilderte Praxis ist auch angesichts § 16 a Abs. 5 Hessisches Meldegesetz nicht zulässig. Diese Norm sieht vor, daß § 12 Abs. 1 S. 1 des Hessischen Datenschutzgesetzes und damit die Bindung an die Erforderlichkeit bis zum 1. Januar 1983 nicht zur Anwendung kommt, soweit die Meldebehörden anderen Behörden, sonstigen öffentlichen Stellen sowie den öffentlich-rechtlichen Religionsgesellschaften personenbezogene Daten durch Weitergabe der Meldescheine übermitteln. Diese Bestimmung will dem technischen Problem Rechnung tragen, daß die Gemeinden einerseits an eine Reihe von Stellen - hier sind namentlich die Statistischen Ämter und die Kirchen zu nennen - die Daten jedes einzelnen Einwohners mitteilen müssen, ein Verfahren zur Beschränkung des Datensatzes auf die jeweils "erforderlichen" Angaben jedoch noch nicht einsatzfähig war und ist. So erhalten die empfangenden Stellen aufgrund dieser Sondersituation mit der jeweiligen Durchschrift mehr Daten des Einwohners als sie für ihre Aufgabenerfüllung eigentlich brauchten. Aber: In all den Fällen, auf die das Gesetz Bezug nimmt, benötigt die Empfängerstelle grundsätzlich die Angaben jedes Bürgers. Jeder Meldeschein ist damit wenigstens zum Teil verwertbar. § 12 Abs. 1 S. 1 HDSG wird m.a.W. durch diese Ausnahmevorschrift nur insoweit außer Kraft gesetzt, als toleriert wird, daß der weitergegebene Datensatz auch "überschüssige" Angaben enthält. Insoweit unterscheidet sich eine Übermittlung nach dieser Vorschrift grundlegend von der Weitergabe aller Meldescheine an die Polizei. Das Ausnahmeverfahren nach § 16 a Abs. 5 Hessisches Meldegesetz ist datenschutzrechtlich ein bedenkliches Zugeständnis an die technische Unzulänglichkeit. Dies ergibt sich schon daraus, daß diese Norm nur bis zu einer bestimmten Frist gelten soll. Sie sollte deshalb nur dann zur Anwendung kommen, wenn dies unumgänglich ist. Wie bereits dargelegt, gilt dies für die Überlassung der Durchschläge an die Kriminalpolizei nicht.

Ein letztes Argument: Der Weitergabe der für das Statistische Landesamt bestimmten Durchschriften an die Polizei steht auch § 11 Abs. 3 des Bundestatistikgesetzes i.V.m. §§ 4, 6 des Gesetzes über die Statistik über die Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes entgegen. Nach dem Bundesstatistikgesetz ist die Übermittlung statistischer Daten nur zulässig, wenn die die jeweilige Statistik begründende Rechtsnorm sie ausdrücklich zuläßt; eine Übermittlung an die Polizei ist jedoch in letztgenanntem Gesetz nicht erwähnt.

4.5.6
Begleituntersuchung zum Test für medizinische Studiengänge

4.5.6.1
Der Fall: Ausschluß von der Teilnahme am Testverfahren

In sog. "harten" numerus clausus-Fächern, wie der Human- und Zahnmedizin, werden die Studienplätze im Rahmen eines besonderen Auswahlverfahrens verteilt (§ 33 HochschulrahmenG). Teil dieses Verfahrens ist das Feststellungsverfahren nach Art. 15 des Staatsvertrages über die Vergabe von Studienplätzen (StaatsV), das darauf abzielt, Fertigkeiten und Kenntnisse des Studienplatzbewerbers zu ermitteln, die für den Studienerfolg von Bedeutung sein können, durch die Schulabschlüsse jedoch nicht nachgewiesen werden. Um den Studienerfolg aufgrund festgestellter Eignung und Fertigkeiten zu prognostizieren, können auch Tests verwandt werden.

Die Kultusministerkonferenz hat beschlossen, für einen Zeitraum von drei Jahren (1979-1982) zum Test für medizinische Studiengänge eine Begleituntersuchung durchführen zu lassen. Diese Begleituntersuchung wird vom "Institut für Test-und Begabungsforschung" der Studienstiftung des Deutschen Volkes durchgeführt. An ihr soll sich jeder Teilnehmer des Testverfahrens gleichzeitig beteiligen. Ihr Ziel soll neben der allgemeinen Evaluation vor allem die Feststellung sein, ob bestimmte Bewerbergruppen durch den Test signifikant bevorzugt oder benachteiligt werden. Eine hessische Studienbewerberin beschwerte sich bei mir darüber, daß der Erhebungsbogen zu dieser Begleituntersuchung die Angabe der persönlichen Registriernummer des Testverfahrens verlangt. Ihre Zweifel an der Anonymität dieser Untersuchung veranlaßten die Petentin, die Eintragung dieser Nummer zu verweigern. Dies hatte zur Folge, daß sie vom Testverfahren - und damit vom Vergabeverfahren im Rahmen der für das Feststellungsverfahren vorgesehenen Quote - ausgeschlossen wurde.

Nach Prüfung der Sach- und Rechtslage mußte ich das Verfahren der Testabnahme einschließlich der Datenverarbeitung bei der Zentralen Vergabestelle (ZVS) sowie beim "Institut für Test- und Begabungsforschung" aus den im folgenden dargelegten Gründen gegenüber dem Hessischen Kultusminister beanstanden.

4.5.6.2
Begleituntersuchung: Teilnahmepflicht als unzulässige Zulassungsvoraussetzung

Die nach § 7 Nr. 1 HDSG erforderliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist § 16 Abs. 5 StaatsV i.V.m. § 23 Abs. 1 VergabeVO.

Die Teilnahme am Feststellungsverfahren ist freiwillig (vgl. § 16 Abs. 3 StaatsV). Die Bewerber sind jedoch verpflichtet, die für die Erprobung und Weiterentwicklung dieses Verfahrens erforderlichen Angaben über ihren Bildungsgang und ihre persönlichen und sozialen Verhältnisse zu machen (§ 16 Abs. 5 StaatsV). Diese Einzelangaben dürfen jedoch nur für Zwecke der Weiterentwicklung und der Erprobung des Feststellungsverfahrens verwendet werden. Stellt ein Teilnehmer seine Daten nicht zur Verfügung, soll er über die für das Feststellungsverfahren vorgesehene Quote nach § 16 Abs. 1 S. 1 Nr. 3 StaatsV nicht zugelassen werden können. Freiwilligkeit der Teilnahme bedeutet hier nur soviel, daß es keine gesetzliche Verpflichtung von Studienplatzbewerbern zur Teilnahme am Feststellungsverfahren gibt. Doch muß sich jeder Bewerber beteiligen, der seine Zulassungschance erhöhen will; so werden im Winter-Semester 1981/82 z.B. 95 Studienplätze an die Testbesten -außerhalb der Landesquoten - vergeben.

Da das Feststellungsverfahren die Funktion der Auswahl und Verteilung der Bewerber auf diese zusätzliche Quote hat, ist es insoweit als eine objektive Zulassungsregelung anzusehen. Dem steht das Recht des Bewerbers - wenn er die sog. "subjektiven Zulassungsvoraussetzungen" (z.B. Abitur) erfüllt - auf Zulassung zum Hochschulstudium seiner Wahl nach Art. 12 Abs. 1 in Verbindung mit Art. 3 Abs. 1 Grundgesetz und dem Sozialstaatsgebot gegenüber (vgl. § 27 Abs. 1 Satz 1 HochschulrahmenG; BVerfG E 33, 332 f.); die Teilnahme ist also aus der Sicht des Studieninteressenten eine Beschränkung des Zulassungsanspruchs. Eine solche Beschränkung ist nach den zu Art. 12 GG entwickelten Grundsätzen des Bundesverfassungsgerichts nur "zur Abwehr nachweisbarer oder höchstwahrscheinlich schwerer Gefahren für ein wichtiges Gemeinschaftsgut" - beim numerus clausus ist das die "Funktionsfähigkeit der Universität als Voraussetzung für die Aufrechterhaltung eines geordneten Studienbetriebs" -sowie nur unter strenger Wahrung des Verhältnismäßigkeitsprinzips zulässig (BVerfG E 33, 339).

Wenn aber Art. 16 Abs. 5 S. 4 StaatsV bestimmt, daß Teilnehmer am Feststellungsverfahren, die sich der gleichzeitigen Begleituntersuchung nicht unterziehen, nicht über die zusätzliche Quote zugelassen werden können, sind Zweifel an der Verfassungsmäßigkeit dieser Bestimmung am Platz. Die Zulassungsbeschränkung wäre dann nicht im Interesse der Verhinderung überhöhter Studentenzahlen an den Hochschulen, sondern lediglich zur Validierung und Weiterentwicklung der Testverfahren erforderlich.

Die Koppelung von Studienplatzvergabe und Begleituntersuchung widerspricht der Rechtsprechung des Bundesverfassungsgerichts, nach der Zulassungsbeschränkungen eine "Auswahl und Verteilung nach sachgerechten Kriterien mit einer Chance für jeden an sich hochschulreifen Bewerber" erfordern (BVerfG E 33,338). Dies gilt auch und gerade für den Test und die Begleituntersuchung, da auch bei diesen Verfahren darauf zu achten ist, daß "die Schwelle (sc. für die Zulassung zum Studium) durch objektiv sachgerechte und individuell zumutbare Kriterien" bestimmt wird (BVerfG E 42, 291, 323 f.).

4.4.6.3
Verfassungskonforme Auslegung: Freiwilligkeit der Beteiligung

Eine verfassungskonforme Auslegung von Art. 16 Abs. 5 StaatsV muß mithin dazu führen, daß im Ergebnis die Studienzulassung nicht von der Beteiligung an der Begleituntersuchung abhängen darf. Diese Interpretation ist auch deshalb zwingend, da der Staatsvertrag selbst in den Art. 15, 16 Nrn. 8 und 9 von der grundsätzlichen Freiwilligkeit der Teilnahme am gesamten Verfahren ausgeht.

Dieser Rechtslage entspricht die Vergabeverordnung, die - anders als der Staatsvertrag - in keiner Bestimmung einen Ausschluß des Bewerbers vom Test-bzw. Vergabeverfahren vorsieht, wenn ein Teilnehmer die Angaben zur Begleituntersuchung verweigert. Anlage 6 Ziff. 2.1 spricht nur davon, daß die Teilnehmer Angaben machen sollen. Weiterhin ist nach § 23 Abs. 4 der Antrag zur Teilnahme am Feststellungsverfahren nur zulässig, wenn der Bewerber ausdrücklich sein Einverständnis mit der Erhebung seiner Daten für das Begleitprojekt und ihrer Verwendung für Evaluierungszwecke erklärt. Datenschutzrechtlich fehlt es somit an einer die Speicherung der persönlichen Angaben der Bewerber, die sie im Begleittest angegeben haben, rechtfertigenden Norm. Sie dürfen m.a.W. nur auf freiwilliger Basis erhoben werden.

Die ZVS hat aber im Gegensatz zu dieser Vorschrift in ihrem vom Bewerber obligatorisch zu benutzenden Formblatt für den Antrag zur Zulassung weder ein Datenfeld für diese Einwilligung noch die erforderliche Aufklärung über den Zweck der Datenverarbeitung im Rahmen der Begleituntersuchung aufgenommen. Darüber hinaus fehlt ein Hinweis auf die Rechtsgrundlage der Erhebung, wie ihn § 11 Abs. 2 HDSG verlangt (vgl. die Datenfelder 337 - 340 des Zulassungsantrags). Auch die Erläuterungen auf S. 21 der ZVS-Information zum Testverfahren weisen nicht auf die Notwendigkeit der Einwilligung hin.

4.5.6.4
Ergebnis und Konsequenzen

Ergebnis und Konsequenzen meiner Stellungnahme lassen sich wie folgt zusammenfassen:

1. Die Verarbeitung der personenbezogenen Daten aller Studienplatzbewerber im Rahmen der Begleituntersuchung war ohne deren ausdrücklich erklärte Einwilligung unzulässig.

2. Die Anforderungen der Datenschutzgesetze müssen in Zukunft eingehalten werden. Dazu habe ich folgende Maßnahmen empfohlen:

- Einholung der Einwilligung des Bewerbers in die Verarbeitung seiner Daten zu Evaluierungszwecken;

- Hinweis auf die Freiwilligkeit der Teilnahme an der Begleituntersuchung;

- Hinweis auf die Rechtsgrundlage für die Datenverarbeitung im Rahmen der Begleituntersuchung und Aufklärung über deren Zweck und Bedeutung.

3. Aufgrund der geschilderten Rechtslage hatte es die Petentin zu Recht abgelehnt, den Erhebungsbogen auszufüllen. Daraus durften ihr nach § 11 Abs. 2 HDSG keine Nachteile entstehen. Ich habe daher ihre "Wiedereinsetzung in den vorigen Stand" angeregt mit der Maßgabe, sie zum Test - ohne Teilnahme am Losverfahren - zuzulassen.

4.5.7
Übermittlung der Daten von Religionslehrern an die Kirchen

Die evangelischen Landeskirchen in Hessen haben den Hessischen Kultusminister unter Berufung auf Art. 57 der Hessischen Verfassung um die Übermittlung von Name, Geburtsdatum, Dienststelle und Lehramt derjenigen Lehrer gebeten, die die Fachlehrbefähigung in evangelischer Religionslehre besitzen. Ihnen geht es um die Feststellung, wer von diesen Lehrern tatsächlich protestantischen Religionsunterricht erteilt. Es gibt begründeten Anlaß zu der Vermutung, daß eine erhebliche Divergenz zwischen der vorhandenen Lehrkapazität und dem Umfang des tatsächlich abgehaltenen Unterrichts in diesem Fach besteht.

In intensiven Gesprächen mit dem Hessischen Kultusminister, dem Hessischen Institut für Bildungsplanung und der Evangelischen Kirche in Hessen und Nassau wurde erörtert, ob und wie dem Informationswunsch der Kirche bei Beachtung der Bestimmungen der Verfassung und des Datenschutzgesetzes entsprochen werden könnte.

Dabei habe ich - auf der Grundlage meiner Ausführungen im 8. Tätigkeitsbericht (2.6) - insbesondere folgende Gesichtspunkte hervorgehoben:

1. Die erbetene Übermittlung aus der Lehrerindividualdatei an die Kirchen richtet sich nach § 12 HDSG. Danach sind bei der Datenübermittlung durch Behörden an die öffentlich-rechtlichen Religionsgesellschaften die Zulässigkeitsvoraussetzungen für die Datenübermittlung innerhalb des öffentlichen Bereichs entsprechend zu beachten. § 12 Abs. 3 HDSG verlangt, daß beim Empfänger ausreichende Datenschutzmaßnahmen getroffen werden. Daß diese Anforderung von den Kirchen in Hessen erfüllt wird, habe ich in meinem 8. Tätigkeitsbericht festgestellt (vgl. 2.6.1).

   1.1 Die Erforderlichkeit zur Aufgabenerfüllung im Sinne des § 12 HDSG kann nur auf dem Hintergrund des verfassungsrechtlichen Verhältnisses zwischen dem Staat und den öffentlich-rechtlichen Religionsgesellschaften beurteilt werden.

   Nach Art. 140 Grundgesetz i.V.m. Art. 137 Abs. 3 Weimarer Verfassung (WV) ordnet und verwaltet jede Religionsgesellschaft ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden Gesetzes. "Die Kirchen sind ungeachtet ihrer Anerkennung als Körperschaften des öffentlichen Rechts dem Staat in keiner Weise inkorporiert, also auch nicht im weitesten Sinne staatsmittelbare Organisationen oder Verwaltungseinrichtungen. Ihre wesentlichen Aufgaben, Befugnisse, Zuständigkeiten sind originäre und nicht vom Staat abgeleitete." (BVerfGE 18, 385 (386); 19, 129 (133f); 42,(312).

   Die Aufgabenerfüllung der staatlichen Verwaltung unterliegt der rechtsstaatlichen Bindung an staatliches Gesetz und Recht, die aus den o.g. Gründen für die Kirchen nicht gelten. Daher fehlt es an einer gemeinsamen rechtlichen Grundlage, wenn personenbezogene Daten aus dem öffentlichen Bereich heraus an eine öffentlich-rechtliche Religionsgesellschaft übermittelt werden. Ob sie diese Daten speichert und weiterverarbeitet und für welche ihrer - selbstbestimmten - Aufgaben sie sie verwendet, ist eine innerkirchliche Angelegenheit, die sie autonom in Unabhängigkeit vom Staat regelt. Staatliche Datenschutzgesetze können insoweit für den innerkirchlichen Bereich keine Geltung beanspruchen.

   1.2 Die Bedeutung des § 12 Abs. 2 HDSG liegt darin, daß die Kirchen in die Regelung der Datenübermittlung innerhalb des öffentlichen Bereichs einbezogen werden, um den Informationsfluß aufrechtzuerhalten, auf den sie nach Art. 140 Grundgesetz i.V.m. Art. 136 ff. Weimarer Verfassung Anspruch erheben können. Darin liegt zugleich aber eine Beschränkung. Die Religionsgesellschaften können von den Behörden und öffentlichen Stellen der Landesverwaltung keine "Amtshilfe" verlangen, wenn die Erfüllung des Ersuchens gegen die staatliche Rechtsordnung verstieße. Die Autonomie der Religionsgesellschaften besteht nur innerhalb der Schranken des für alle geltenden Gesetzes (Art. 137 Abs. 3 WV). Diese Schrankenformel ist "heute die Basis für eine Konkordanz zwischen staatlicher und kirchlicher Ordnung, die es gestattet, auf beiden Seiten davon auszugehen, daß staatliche Gesetze nicht die den Kirchen wesentlichen eigenen Ordnungen beeinträchtigen, und daß kirchliche Gesetze nicht die für den Staat unabdingbare Ordnung kränken werden" (BVerfGE 42, 312/340). Zum richtigen Verständnis einer partnerschaftlichen Kooperation auf dieser Grundlage gehört die Bereitschaft der Kirche, die Pflicht der vollziehenden Gewalt zu respektieren und die Grundrechte zu achten.

2. Unter Berücksichtigung dieser Prinzipien sowie aufgrund der Artikel 4 und 7 Grundgesetz, 57 und 58 Satz 2 Hessische Verfassung ist die Frage zu beantworten, ob das Land Hessen die persönlichen Daten der Lehrer mit Fachlehrbefähigung an die Kirche weitergeben darf, ohne zuvor deren Einwilligung einzuholen.

   2.1 Konstitutiv für die Befugnis einzelner Lehrer, tatsächlich im Fach Religion zu unterrichten, ist nicht die aufgrund staatlicher Prüfungen erworbene Fachlehrbefähigung, sondern die durch die öffentlich-rechtlichen Religionsgesellschaften erteilten Bevollmächtigungen (vgl. den Religionsunterrichts-Erlaß des Hessischen Kultusministers vom 18. November 1976, Amtsblatt S. 655).

   Folgerichtig ist in diesem Erlaß unter Abschnitt II Ziff. 2 S. 3 eine gegenseitige Information im Rahmen eines partnerschaftlichen Zusammenwirkens zwischen Staat und Kirche vorgesehen, soweit die Erteilung oder der Widerruf der **kirchenrechtlichen** Bevollmächtigung in Frage stehen. Daraus folgt zunächst, daß gegen eine Mitteilung der Daten derjenigen Lehrer an die Kirche, die tatsächlich Religionsunterricht mit kirchlicher Bevollmächtigung geben, keine grundsätzlichen Bedenken bestehen.

2.2 Dagegen ist die Mitteilung der Daten von Lehrern, die zwar die staatliche Fachlehrbefähigung, nicht aber die kirchliche Bevollmächtigung besitzen, ohne deren Einwilligung aus verfassungsrechtlichen Gründen bedenklich. Aus Art. 7 Abs. 3 S. 3 GG und Art. 58 S. 2 Hessische Verfassung wird ein negatorisches Grundrecht des Lehrers gegen eine staatliche Verpflichtung zum Religionsunterricht abgeleitet. In Verbindung mit der "negativen Bekenntnisfreiheit" aus Art. 4 GG kann diese Grundrechtsposition des Betroffenen durch die Weitergabe seiner Daten an die Kirche beeinträchtigt werden, insbesondere wenn er zwischenzeitlich aus der Kirche ausgetreten oder Atheist geworden ist. Dies hat zur Konsequenz, daß für diese Gruppe von Lehrern die Einwilligung in die Datenübermittlung erforderlich ist. Gegen eine Bekanntgabe statistisch aggregierter Daten über vorhandene Lehrkapazitäten aus der Lehrerindividualdatei ist dagegen nichts einzuwenden.

4.5.8
Offenbarung von Sozialdaten an Kreditinstitute

4.5.8.1
Überweisungsgrund auf Bankbelegen

Durch Presseberichte und Anfragen wurde ich auf folgendes Problem aufmerksam gemacht: Sozialhilfeempfänger, die ihre Leistung vom Sozialamt auf ihr Bankkonto überwiesen erhalten, mußten feststellen, daß der Überweisungsbeleg die Angabe "Sozialhilfe" bzw. eine weitere, detaillierte Aufschlüsselung des Betrags enthielt. Die Bank des Leistungsbeziehers erhält somit von der Inanspruchnahme der Sozialhilfe Kenntnis. Die wirtschaftliche Lage ihres Kunden wird ihr damit offengelegt, seine Bonität leidet Schaden, negative Konsequenzen drohen etwa bei der Beantragung eines Kredits.

Bedenkt man, daß nicht nur in großem Umfang die Sozialhilfe, sondern auch viele andere Sozialleistungen bargeldlos abgewickelt werden, wird die datenschutzrechtliche Problematik dieser Praxis ohne weiteres deutlich. Dabei wäre es unredlich, das Problem unter Berufung auf ein aufgeklärtes Verständnis von Aufgabe und Funktion des Systems sozialer Sicherung zu bagatellisieren, nach dem der Bezug von Sozialleistungen keinen diskriminierenden Charakter hat. In der Realität ist dies - leider - nach wie vor anders.

Grundlage der rechtlichen Würdigung ist § 69 SGB X: Mit der Angabe des Überweisungsgrundes "Sozialhilfe", erst recht mit weiteren Hinweisen zum Verwendungszweck, gibt das Sozialamt den Kreditinstituten personenbezogene Daten der Leistungsempfänger bekannt. Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung von Sozialdaten jedoch (nur) dann und insoweit zulässig, als sie für die Erfüllung der gesetzlichen Aufgabe des Sozialamtes, hier mithin für die Abwicklung der Auszahlung der Sozialhilfe, erforderlich ist. Ob diese "Erforderlichkeit" vorliegt, beurteilt sich im Datenschutzrecht nach der faktischen Möglichkeit, Alternativen zu finden, bei denen die Übermittlung personenbezogener Daten in geringerem Umfang stattfinden oder gänzlich überflüssig werden kann.

In Hessen ist dabei von folgender Sachlage auszugehen:

- Der größte Teil der Kreise und kreisfreien Städte in Hessen bedient sich zur Berechnung, Bescheidschreibung und Überweisung der Sozialhilfe der Auftragsdatenverarbeitung durch die Kommunalen Gebietsrechenzentren (landeseinheitliches Verfahren HES-SIAS I).

- Dieses Verfahren HES-SIAS I sieht die Möglichkeit vor, daß der einzelne Sachbearbeiter des jeweiligen Sozialamtes manuell einen Text vorgibt, der vollständig auf den Überweisungsbeleg für den Hilfeempfänger übernommen wird. Den Sozialämtern ist es somit unbenommen, die Verwendungszweckangabe neutral, d.h. ohne Hinweis auf Art und Einzelheiten der gewährten Leistung zu gestalten. Möglich ist beispielsweise, wie von einem Eingeber vorgeschlagen, statt der Angabe "Sozialhilfe" die Formel "betreffend Ihren Antrag vom ..." zu verwenden. Erst wenn der Sachbearbeiter keinerlei Mitteilung zum Überweisungsgrund macht, wird auf dem Bankbeleg automatisch die Angabe "Sozialleistung" (nach einer zwischenzeitlich erfolgten Änderung also nicht mehr "Sozialhilfe") ausgedruckt. Von der programmtechnischen Seite her besteht somit kein Zwang, bei der bargeldlosen Zahlung Sozialdaten der Leistungsempfänger zu offenbaren.

Doch kann in vielen Fällen auf nähere Angaben zum Verwendungszweck auf den Bankbelegen nicht verzichtet werden. Fachleute aus den Sozialämtern führen hierfür folgende einleuchtende Argumente an: Wenn ein Bürger z.B. mehrere unterschiedliche Sozialleistungen beantragt hat oder diese in verschiedenen Raten ausgezahlt werden, spielt der Gesichtspunkt der Klarheit für den Empfänger eine wichtige Rolle. Dies gilt auch angesichts der Tatsache, daß manche Hilfeempfänger wegen ihres Gesundheitszustandes, ihres Bildungsstandes oder ähnlicher Gründe ohnehin Schwierigkeiten beim Umgang mit Behörden haben. Auch Gründe der Beweisbarkeit bei

gerichtlichen Auseinandersetzungen mit Antragstellern können für eine genaue Aufschlüsselung auf dem Bankbeleg sprechen. Diese Gründe legitimieren im Sinne der "Erforderlichkeit" des § 69 Abs. 1 Nr. 1 SGB X auch den unvermeidlichen Nebeneffekt, daß den Kreditinstituten Sozialdaten "offenbart" werden. Die Verantwortung für die geringstmögliche Durchbrechung des Sozialgeheimnisses verbleibt, da der Überweisungsgrund der automatisierten Verarbeitung variabel vorgegeben werden kann (s.o.), beim Leistungsträger, konkret also bei den Kommunen bzw. Sozialämtern.

Die Mißbrauchsgefahr für den einzelnen Hilfeempfänger liegt bei dieser Praxis auch weniger in der bloßen Kenntnisnahme durch den einzelnen Sachbearbeiter der Bank. Vielmehr kommt es darauf an, sicherzustellen, daß Banken bzw. Sparkassen ihre Kenntnis vom Sozialhilfebezug nicht zu anderen Zwecken verwenden oder derartige Daten gar an Kreditschutzorganisationen, Auskunfteien o.ä. übermitteln. Das Gesetz ist hier eindeutig: Sozialdaten dürfen von den sie empfangenden Stellen ausschließlich zu dem Zweck verwendet werden, zu dem sie ihnen befugt offenbart worden sind, hier also zur Auszahlung der Sozialhilfe (§ 78 Satz 1 SGB X). Ob diese gesetzliche Forderung eingehalten wird, kann der Hessische Datenschutzbeauftragte jedoch nicht selbst nachprüfen, da sich seine Überwachungskompetenz weder auf privatrechtliche noch auf öffentlich-rechtliche Kreditintitute erstreckt. Ich habe daher den Hessischen Innenminister gebeten, die Regierungspräsidenten als Aufsichtsbehörden für den Datenschutz bei Banken und Sparkassen auf diese Sach- und Rechtslage und ihre Einbeziehung bei Datenschutzkontrollen hinzuweisen.

4.5.8.2
Einholung von Auskünften bei Banken durch Sozialhilfeträger

Kreditinstitute erhalten noch in einem anderen Zusammenhang Kenntnis zumindest davon, daß einer ihrer Kunden einen Antrag auf Sozialhilfe gestellt hat, nämlich dann, wenn das Sozialamt über den Kontostand bzw. die Kontobewegungen des Antragstellers Auskunft einholt. Dies geschieht zur Feststellung, ob der Antragsteller nicht über Einkommen bzw. Vermögen verfügt, das den Anspruch auf Sozialhilfe ausschließt oder verringert. Für die Einholung dieser Informationen und die dafür erforderliche Einwilligung des Betroffenen hat der Deutsche Gemeindeverlag ein Formblatt entwickelt, das offensichtlich bundesweit in zahlreichen Kommunen verwandt wurde bzw. wird. Ich habe diesen Vordruck wegen Verstoßes gegen den Sozialdatenschutz bemängelt, weil er nicht nur die für die Befreiung vom "Bankgeheimnis" notwendigen Daten enthält (Name, Kontonummer), sondern weitere Angaben über den Hilfeempfänger, die mit der Übersendung des ausgefüllten Formulars zwangsläufig der Bank bzw. Sparkasse bekannt werden. Hier fehlt es an der "Erforderlichkeit" der Weitergabe von Sozialdaten im Sinne des § 69 Abs. 1 Nr. 1 SGB X.

Ich habe daraufhin ein auf die wesentlichen Daten reduziertes Formular entworfen und dem Landeswohlfahrtsverband Hessen - als überörtlichem Träger der Sozialhilfe - zur Verwendung vorgeschlagen. Dieser hat meine Anregung unverzüglich aufgegriffen und die Empfehlung, entsprechend zu verfahren, an alle Kreise und kreisfreien Städte gerichtet.

Dieser Fall macht erneut den wichtigen datenschutzrechtlichen Aspekt der Gestaltung und Verwendung von Formularen deutlich. Vordrucke sind ein unentbehrliches Hilfsmittel für den rationellen und effizienten Verwaltungsvollzug; ständig werden neue Formulare eingeführt bzw. alte abgeändert. Die Datenschutzgesetze verlangen, daß ihre Anforderungen beim Entwerfen von Formblättern von Anfang an einbezogen werden. Konkret heißt das für die Verwaltung, dafür zu sorgen, daß nur das für die Aufgabenerfüllung notwendige Minimum an Angaben auf dem Vordruck angeführt wird. Dies gilt vor allem für die Behörden und Stellen, die Vordrucke für einen großen Adressatenkreis entwickeln und überörtlich zur Verwendung vorschreiben oder empfehlen.

Wiesbaden, den 15. Januar 1982

Prof. Dr. Simitis

5. Materialien

5.1
Erlaß des Hessischen Ministers des Innern vom 13. Juni 1981 (StAnz. 25/1981 S. 1262)

Betr.: Übermittlung von personenbezogenen Daten an öffentliche Forschungseinrichtungen aus Dateien öffentlicher Stellen

Werden personenbezogene Daten aus Dateien öffentlicher Stellen an Hochschulen oder andere öffentliche Einrichtungen mit der Aufgabe wissenschaftlicher Forschung übermittelt, dann richtet sich die Zulässigkeit der Übermittlung nach § 15 des Hessischen Datenschutzgesetzes (HDSG), soweit keine besondere Rechtsvorschrift (wie § 75 Sozialgesetzbuch X) vorgeht.

Die Übermittlung ist zulässig, wenn die Betroffenen eingewilligt haben oder wenn ihre schutzwürdigen Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden (§ 15 Abs. 1 Satz 2 HDSG).

Einheitliche Grundsätze für die Feststellung, daß schutzwürdige Belange nicht beeinträchtigt werden, lassen sich für die beiden folgenden Fallgruppen aufstellen:

I.

Übermittlung von Namen und Anschrift zur Durchführung von Umfragen

Für bestimmte Forschungsvorhaben sind Befragungen ausgewählter Personengruppen erforderlich, deren Namen und Anschriften die öffentlichen Forschungseinrichtungen von den Einwohnermeldeämtern oder anderen öffentlichen Stellen anfordern. Diese Stellen dürfen Name und Anschrift auch ohne Einwilligung des Betroffenen an die Forschungseinrichtung übermitteln, wenn diese versichert, daß folgende Grundsätze von ihr beachtet werden:

1. Der Betroffene wird über Zweck und Form des Forschungsvorhabens aufgeklärt.

2. Der Betroffene wird über die Freiwilligkeit der Teilnahme an der Befragung unterrichtet und darauf aufmerksam gemacht, daß ihm aus der Verweigerung der Teilnahme keine Nachteile entstehen.

3. Die Einwilligung des Betroffenen in die Erhebung und Speicherung seiner personenbezogenen Daten durch die Forschungseinrichtungen wird schriftlich eingeholt. Sollen die Daten an Dritte weitergegeben werden, so ist hierfür eine gesonderte schriftliche Einwilligung des Betroffenen erforderlich.

4. Die Daten derjenigen Betroffenen, die die Teilnahme an der Befragung verweigern, werden unverzüglich gelöscht.

II.

Übermittlung personenbezogener Daten bei anschließender Anonymisierung

Für bestimmte Forschungsvorhaben werden bestimmte personenbezogene Daten derart verändert, daß sie sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen (Anonymisierung).

Wird die Anonymisierung bereits vor der Übermittlung bei der übermittelnden Stelle durchgeführt, dann findet das Datenschutzgesetz auf die Übermittlung der anonymisierten Daten keine Anwendung mehr. Wird die Anonymisierung erst von der Forschungseinrichtung vorgenommen, etwa weil die übermittelnde Stelle dazu nicht in der Lage ist, dann beeinträchtigt die Übermittlung der noch personenbezogenen Daten keine schutzwürdigen Belange des Betroffenen, wenn die Forschungseinrichtung sicherstellt, daß die Daten unverzüglich nach der Übermittlung anonymisiert werden und keiner anderen Verwendung zugeführt werden.

In allen Fällen hat die Forschungseinrichtung zu gewährleisten, daß die mit dem Forschungsvorhaben befaßten Personen auf das Datengeheimnis verpflichtet sind und daß alle zur Datensicherung erforderlichen Maßnahmen getroffen sind.

Dieser Erlaß ergeht im Einvernehmen mit dem Hessischen Kultusminister.

5.2
Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherung bei den ADV-Einrichtungen der hessischen Hochschulen

§ 1 Aufgabe

Die nachstehenden Vorschriften regeln die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung in den ADV-Einrichtungen der Hochschulen auf der Grundlage des Hessischen Datenschutzgesetzes (HDSG) und der sonstigen Rechtsvorschriften zum Schutz personenbezogener Daten.

§ 2 Geltungsbereich

(1) Die Hochschule führt eine Liste über ihre ADV-Einrichtungen mit Angaben über die

- für die ADV-Einrichtung verantwortliche Person
- Art der ADV-Einrichtung
- Zulassung zur Verarbeitung personenbezogener Daten

(2) Für ADV-Einrichtungen, die zur Verarbeitung personenbezogener Daten zugelassen sind, enthält die unter § 2 (1) genannte Liste darüberhinaus Angaben, die die innerbetriebliche Organisation darstellen sowie die dort beschäftigten Mitarbeiter, deren Befugnisse und Verantwortlichkeiten.

§ 3 Sicherheitsbereich

ADV-Einrichtungen nach § 2 (2) sind in einem Sicherheitsbereich unterzubringen. Zum Sicherheitsbereich gehören alle Räumlichkeiten, in denen personenbezogene Daten und dazugehörige Programme verarbeitet oder aufbewahrt werden. Die Hochschule kann weitere Räume dem Sicherheitsbereich zuordnen.

§ 4 Schutz- und Sicherungsmaßnahmen

(1) Für den Sicherheitsbereich sind Zu- und Abgangskontrollen durchzuführen. Die Einzelheiten des Zu- und Abgangs, die Beaufsichtigung von Besuchergruppen sind in besonderen Dienstanweisungen festzulegen.

Insbesondere sind folgende Maßnahmen zu realisieren: Die Zugänge zu den Räumen des Sicherheitsbereichs sind ständig verschlossen zu halten. Zutritt haben grundsätzlich nur die hierfür befugten Mitarbeiter. Andere Mitarbeiter haben nur Zutritt, wenn ihre Anwesenheit zur Erledigung von dienstlichen Aufgaben erforderlich ist. Dritte dürfen sich in den Räumen des Sicherheitsbereichs nur unter Aufsicht der hierfür Verantwortlichen aufhalten. Ausnahmen werden vom jeweils Verantwortlichen gemeinsam mit dem Referenten für den Datenschutz geregelt.

(2) Es ist eine Auftragskontrolle durchzuführen.

Die speichernde Stelle hat bei einer Vergabe von Datenverarbeitungsaufträgen an Dritte sicherzustellen, daß der Auftragnehmer die Bestimmungen des Hessischen Datenschutzgesetzes und der sonstigen Verwaltungsvorschriften zum Schutz personenbezogener Daten beachtet und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 10 (1) HDSG) sorgfältig auszuwählen.

(3) Es ist eine Transportkontrolle durchzuführen.

Die speichernde Stelle ist für den Datentransport verantwortlich. Sie legt die Datenschutz- und Datensicherungsmaßnahmen für den Datentransport fest, auch soweit Dritte mit dem Transport beauftragt werden.

(4) Bei Datenfernverarbeitung trägt die für die ADV-Einrichtung verantwortliche Person auch die Verantwortung für solche Kommunikationswege, die zwischen ihren Datenverarbeitungsgeräten installiert sind, soweit nicht andere Dienststellen zuständig sind. Für andere Kommunikationswege trägt der Auftraggeber bzw. Benutzer der Datenverarbeitungseinrichtung die Verantwortung. Er hat sich über die verschiedenen Kommunikationswege und -möglichkeiten zu informieren und die geeigneten auszuwählen.

(5) Es ist eine Eingabekontrolle durchzuführen.

Die speichernde Stelle protokolliert die Eingabe von personenbezogenen Daten so, daß nachträglich überprüft und festgestellt werden kann, zu welcher Zeit und von wem diese eingegeben worden sind.

(6) Es ist eine Speicherkontrolle durchzuführen. Es sind technische und organisatorische Maßnahmen zu ergreifen, die sicherstellen, daß die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten und deren Verarbeitungsprogramme verhindert werden. Verstöße gegen Zugriffsregelungen sollen angezeigt werden und protokolliert werden.

(7) Es ist eine Zugriffskontrolle einzuführen. Jeder Benutzer einer Datenverarbeitungseinrichtung erhält eine Benutzerkennung. Es sind Maßnahmen zu treffen, die die Überprüfung der Benutzerkennung sicherstellen. Die Zugriffe auf personenbezogene Daten und deren Verarbeitungsprogramme sollen auf das notwendige Maß (zeitlich, örtlich...) beschränkt werden. Einzelheiten regelt die Hochschule durch eine Dienstanweisung.

(8) Es ist eine Benutzerkontrolle durchzuführen.

Der Kreis der Benutzer der ADV-Einrichtung muß protokolliert werden.

(9) Es ist eine Übermittlungskontrolle durchzuführen, es ist zu gewährleisten, daß angezeigt und protokolliert wird, wann welchen Stellen personenbezogene Daten übermittelt werden.

§ 5 Protokolle

Die speichernde Stelle in Zusammenarbeit mit den Selbstverwaltungs- und weiteren gesetzlichen Organen regelt die Berechtigung und den Umfang des Zugriffs auf die Protokollierung nach § 4 (4, 5, 7, 8) und § 6 (2), § 8, § 9 der Richtlinien.

§ 6 Besondere Pflichten des Benutzers

(1) Der Benutzer zeigt dem für die ADV-Einrichtung Verantwortlichen und dem Referenten für den Datenschutz die Verarbeitung personenbezogener Daten an.

(2) Grundsätzlich hat der Benutzer als Verarbeiter personenbezogener Daten

a) rechtzeitig mit dem Verantwortlichen für die ADV-Einrichtung die Möglichkeiten zur Einhaltung der Datenschutz- und Datensicherungsregeln zu erörtern,

b) bei bei Mißbrauchsvermutung den Verantwortlichen für die ADV-Einrichtung sofort in Kenntnis zu setzen,

c) bei Vermutung von Schwachstellen den Verantwortlichen für die ADV-Einrichtung sofort zu unterrichten,

d) bei bei der Feststellung von Datenschutzverletzungen mitzuarbeiten, insbesondere Unterlagen und Dateien dem Referenten für den Datenschutz und dem Verantwortlichen für die ADV-Einrichtung zur Verfügung zu stellen,

e) für für die Rückgabe von Programmen und Ablaufprotokollen, von zur Eingabe verwendeten Datenträgern sowie von erzeugten Ausgaben technische Maßnahmen wie Schließfächer, die sicherstellen, daß kein Unbefugter von den Unterlagen Kenntnis erhält von dem Verantwortlichen für die ADV-Einrichtung anzufordern, zu benutzen oder die Datenträger und alle mit der Verarbeitung personenbezogener Daten zusammenhängenden Unterlagen persönlich in Empfang zu nehmen,

f) die Ein-und Rückgabe von wiederverwendbaren Datenträgern, wie Magnetbändern, Wechselplatten, Stapel, Disketten und Magnetkassetten durch Quittung zu bestätigen. Er hat sich dabei zu legitimieren,

g) Erfassungsbelege, Lochkarten, Programmlisten und Dokumentationen sind, wenn sie nicht mehr benötigt werden, zu vernichten. Die Vernichtung ist zu protokollieren.

(3) Darüberhinaus haben die Benutzer alle angebotenen Schutzvorkehrungen wahrzunehmen und auch angemessene Sicherheitsvorkehrungen zu treffen, soweit die Daten und die Verarbeitungsvorgänge dies erfordern.

(4) Die Weitergabe von Zugriffsrechten des einzelnen Benutzers von den ihm zugeteilten Datenträgern an Dritte ist nur im Rahmen des HDSG zulässig.

§ 7 Grundsätze beim Einsatz von ADV-Verfahren

(1) Bibliotheken für Quellen, ausführbare Programme, Prozeduren sowie Dateien sind für den Produktions- und Testbereich getrennt zu führen.

(2) Programme und personenbezogene Daten sind so zu sichern und auszulagern, daß sie rekonstruierbar sind. Die Art und Organisation der Sicherung und Auslagerung ist schriftlich zu regeln. Für das Auslagern, die Erstellung von Sicherungskopien bzw. Versionen etc. sind entsprechende Richtlinien zu erlassen. Es muß sichergestellt sein, daß am Ort der Auslagerung die Daten vor unberechtigtem Zugriff geschützt sind.

(3) Bei der Verarbeitung von personenbezogenen Daten ist zu gewährleisten, daß Arbeitsergebnisse, Dateien sowie Steueranweisungen, die Informationen über die Kontrollmechanismen beinhalten, nur Personen zur Kenntnis gelangen können, die nach § 2 (2) oder durch Einzelauftrag dazu berechtigt sind.

(4) Datenträger werden gemäß Arbeitsanweisungen gelöscht. Auszuliefernde Datenträger mit personenbezogenen Daten sind vor dem Beschreiben grundsätzlich physikalisch vollständig zu löschen. Arbeitsunterlagen und Datenträger mit personenbezogenen Daten, die weder auszuliefern noch aufzubewahren sind, werden so vernichtet bzw. gelöscht, daß ihr Inhalt nicht mehr rekonstruiert werden kann. Dies ist so zu organisieren, daß dabei eine Kenntnisnahme der Daten durch Unbefugte ausgeschlossen ist. Soweit Datenträger keinem Eigner zugeordnet sind oder von einem Eigner freigegeben werden, sind diese zu löschen.

§ 8 Maschinenbetrieb

Nur die mit dem Maschinenbetrieb beschäftigten Personen führen die maschinellen Arbeiten aus. Es ist ein ausführliches Maschinentagebuch insbesondere mit Angaben über Zeiten der Unterbrechung und Wartung sowie den Namen der Operatoren pro System und Schicht zu führen und die Datenverarbeitungsaufträge und ihre Auftraggeber sind zu protokollieren.

Die Durchführung von Wartungsarbeiten und sonstigen Arbeiten im Maschinenbereich (z.B. Reinigung, Wartung/Reparatur der Klimaanlage) ist auf einem Arbeitsauftrag zu bestätigen und im Maschinentagebuch zu vermerken.

§ 9 Datenarchiv

Alle von der EDV-Einrichtung verwalteten Datenträger sind in einem Datenarchiv zu halten. Das Datenarchiv gehört zum Sicherheitsbereich. Für den ganzen Bereich des Archivs ist § 4 (8, 9) entsprechend anzuwenden.

§ 10 Gebäudesicherung

Die erforderlichen Gebäude-, Raum- und/oder Gerätesicherungsmaßnahmen sind auf der Grundlage eines Gutachtens des Hessischen Landeskriminalamtes zu realisieren.

§ 11 Verpflichtung auf das Datengeheimnis

(1) Über die in § 2 (2) bezeichneten Mitarbeiter hinaus sind alle mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiter oder in deren Auftrag bei der Datenverarbeitung tätigen Personen bei der Aufnahme ihrer Tätigkeit auf die Einhaltung des Datengeheimnisses zu verpflichten, sofern diese Verpflichtung nicht bereits durch eine andere Stelle erfolgt ist. Ein Auszug aus dem Hessischen Datenschutzgesetz ist auszuhändigen. Die Verpflichtung kann mit derjenigen nach den Verpflichtungsgesetzen verbunden werden.

§ 12 Referent für den Datenschutz gemäß § 27 Hessisches Hochschulgesetz

(1) Der Referent für den Datenschutz berichtet unmittelbar dem Präsidenten der Hochschule. Er ist für alle Grundsatzfragen des Rechts der Datenverarbeitung zuständig. Er entscheidet insbesondere über die Zulassung einer ADV-Einrichtung zur Speicherung und Verarbeitung personenbezogener Daten. Er wirkt außerdem bei folgenden Aufgaben mit:

- Beratung und Schulung auf dem Gebiet von Datenschutz und Datensicherung,
- Überwachung der Durchführung von Datenschutzmaßnahmen, die sich auf die ADV-Einrichtung auswirken,
- Erstellung und Fortschreibung von Vorschriften für Datenschutz und Datensicherung, Überwachung der Einhaltung dieser Vorschriften,
- Entscheidungen bezüglich Datenschutz und Datensicherung zum Datensicherungssystem der ADV-Einrichtung.

(2) Dem Referenten für den Datenschutz steht ein Empfehlungs- und Kontrollrecht unmittelbar gegenüber allen Funktionsträgern zu. Er ist verpflichtet, der Durchführung einzelner Maßnahmen, die nach seiner Ansicht gegen Datenschutzvorschriften verstoßen, zu widersprechen. Zur Erfüllung seiner Aufgaben ist ihm

- Zutritt in alle Diensträume zu gewähren,
- Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme.

(3) Der Referent für den Datenschutz ist bei der Erfüllung seiner Aufgaben durch den Verantwortlichen für die ADV-Einrichtung zu unterstützen.

(4) Die weiteren Einzelheiten können in einer besonderen Dienstanweisung geregelt werden.

5.3
Richtlinien für die Tätigkeit der Schulpsychologen in der Abteilung schulpsychologischer Dienst im Staatlichen Schulamt (Entwurf)

I.
II.
III.

1. Sofern Schulpsychologen Untersuchungen durchführen, zu deren Teilnahme die betroffenen Schüler aufgrund eines Gesetzes verpflichtet sind, bedürfen diese keines Einverständnisses der Betroffenen.
2. Sofern Schulpsychologen auf Anforderung von Lehrern, Schulleitern, Schulärzten oder Schulaufsichtsbehörden tätig werden und die betroffenen Schüler zur Teilnahme an den erforderlichen Untersuchungen nicht verpflichtet sind, können diese nur durchgeführt werden, wenn die Erziehungsberechtigten oder die volljährigen Schüler eine Einverständniserklärung darüber abgeben, daß sie mit der Untersuchung und damit einverstanden sind, daß deren Ergebnis in dem erforderlichen Umfang den in Satz 1 Genannten bekanntgegeben werden. Die Einverständniserklärung ist vor Beginn der Untersuchung abzugeben.

3. Sofern Schulpsychologen auf Wunsch von Erziehungsberechtigten oder volljährigen Schülern tätig werden, ist eine Weitergabe von Ergebnissen der Untersuchung an Dritte nur mit schriftlichem Einverständnis der Betroffenen und nur in dem von diesen festzulegenden Umfang zulässig.

4. Sofern Schulpsychologen auf Wunsch von minderjährigen Schülern tätig werden, ist eine erste Beratung zulässig. Werden darüber hinaus weitere Maßnahmen erforderlich, sind diese nur zulässig, wenn eine schriftliche Einverständniserklärung der Erziehungsberechtigten vorliegt.

IV.

1. In den Fällen des Abschnitt III Nr. 1 sind die Schulpsychologen verpflichtet, Vorgesetzten und Schulaufsichtsbehörden auf Anforderung alle erforderlichen Auskünfte zu erteilen und erforderlichenfalls auch Akteneinsicht zu gewähren.

2. In den Fällen des Abschnitt III Nr. 2 sind die Schulpsychologen verpflichtet, Vorgesetzten und Schulaufsichtsbehörden auf Anforderung alle Auskünfte zu erteilen, die von der Einverständniserklärung der Betroffenen umfaßt werden. Eine Akteneinsicht ist nicht zu gewähren, wenn in den Akten Vorgänge enthalten sind, die nicht von der Einverständniserklärung der Betroffenen erfaßt werden.

3. In den Fällen des Abschnitt III Nr. 3 und 4 dürfen Vorgesetzten und Schulaufsichtsbehörden nur dann Auskünfte erteilt werden und Akteneinsicht gewährt werden, wenn eine schriftliche Einverständniserklärung der Betroffenen vorliegt.

4. Unabhängig von vorstehenden Regelungen ist der Schulpsychologe im Rahmen der Dienstaufsicht verpflichtet, Vorgesetzten und Schulaufsichtsbehörden allgemein Auskunft über Art, Umfang und Dauer seiner Tätigkeit zu erteilen; Angaben über dem Schutz von Persönlichkeitsrechten und dem Datenschutz unterliegende Sachverhalte sind in diesen Fällen nicht zulässig.

V.

1. Der Schulpsychologe gewinnt Untersuchungsergebnisse durch Exploration, psychodiagnostische Verfahren und Verhaltensbeobachtungen. Er ist bei seiner Tätigkeit im Hinblick auf den sachlichen Inhalt an Weisungen nicht gebunden. In den Fällen des Abschnitts III Nr. 1 ist der Schulpsychologe an Weisungen der Schulaufsichtsbehörde gebunden. Im übrigen bleiben die allgemeinen Weisungsbefugnisse des Abteilungsleiters und des Hauptabteilungsleiters unberührt.

2. Über die Heranziehung oder die Anwesenheit Dritter entscheidet in den Fällen des Abschnitts III Nr. 1 der Schulpsychologe; in den übrigen Fällen bedarf dies der Zustimmung der Erziehungsberechtigten oder der volljährigen Schüler.

VI.

1. . . .

2. Mit anderen Beratungseinrichtungen, z.B. mit den Vertretern der Schulgesundheitsfürsorge, der Familienfürsorge, der Erziehungsberatung, der Drogenberatung und der Berufsberatung arbeitet der Schulpsychologe erforderlichenfalls im Rahmen seiner Aufgaben zusammen. Für Auskünfte an diese Einrichtungen oder an andere Dritte gilt Abschnitt IV entsprechend.

3. Für Aussagen und gutachtliche Äußerungen vor Gericht bedarf der Schulpsychologe der Aussagegenehmigung oder der Zustimmung des Behördenleiters.

VII.

1. Alle wesentlichen Ergebnisse der schulpsychologischen Tätigkeit hält der Schulpsychologe in Aktenunterlagen und in einer Fallkartei fest.

2. Fallkartei, Testmaterial und alle dazugehörigen Unterlagen sind unter Verschluß zu halten. Sie sind bis zum Ablauf von 5 Jahren nach Beendigung der Schulpflicht aufzubewahren; danach sind sie als Vorgänge vertraulichen Inhalts zu vernichten. Dies gilt auch für Vorgänge, die vor der Einrichtung der Abteilungen Schulpsychologischer Dienst entstanden sind.

3. . . .

5.4
Rechtsvorschriften und veröffentlichte Erlasse zum Datenschutz und zur Datensicherung für den öffentlichen Bereich in Hessen (Auswahl)

1. Rechtsvorschriften

1.1
des Landes Hessen

1. Hessisches Datenschutzgesetz (HDSG) vom 31. Januar 1978 (GVBl. I S. 96 - zuletzt geändert durch Nr. 2)
2. Gesetz zur Änderung des Hessischen Datenschutzgesetzes vom 14. Oktober 1980 (GVBl. I S. 377) betr. Abschaffung der Gebührenpflicht für Auskünfte gem. § 18 HDSG
3. Hessisches Meldegesetz vom 22. September 1960 (GVBl. I S. 201), zuletzt geändert durch Gesetz vom 3. November 1981 (GVBl. I S. 385) - § 16 a -
4. Hessisches Krankenhausgesetz vom 4. April 1973 - § 14 - (GVBl. I S. 145)
5. Hessisches Hochschulgesetz (HHG) vom 6. Juni 1978 i.d.F. vom 10. Oktober 1978 - § 27 - (GVBl. I S. 391)
6. Hessische Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten vom 1. November 1978 (GVBl. I S. 553)
7. Hessische Verordnung über die von dem Hessischen Datenschutzbeauftragten zu führenden Dateienregister vom 8. Dezember 1978 (GVBl. I S. 682).

1.2
des Bundes

(Auswahl der wichtigsten Gesetze mit bereichsspezifischen Datenschutzregelungen)

1. Gesetz über Personalausweise, zuletzt geändert durch Gesetz vom 6. März 1980 (BGBl. I S. 270) - § 3 -
2. Gesetz über die Statistik für Bundeszwecke vom 14. März 1980 - § 11 - (BGBl. I S. 289)
3. Melderechtsrahmengesetz vom 16. August 1980 (GVBl. I S. 1429)
4. Sozialgesetzbuch - Zehntes Buch - vom 18. August 1980 - §§ 67 ff. - (BGBl. I S. 1469).

2. Erlasse in Hessen

1. Erlaß über wissenschaftliche Untersuchungen im Schulbereich (hier: Antragstellung) vom 4. Mai 1977 (Amtsblatt des Hessischen Kultusministers S. 256)
2. Erlaß über Angaben über Schüler gegenüber Außenstehenden vom 10. Oktober 1977 (Amtsblatt des Hessischen Kultusministers S. 565)
3. Vorläufige Verwaltungsvorschrift zur Landeshaushaltsordnung (VV -LHO) zu § 79 LHO Anlage 2:

   Bestimmungen über die Verfahrenssicherheit bei der Verwendung automatischer Datenverarbeitungsanlagen (ADV-Anlagen) im Haushalts-, Kassen- und Rechnungswesen und für die Übernahme des Inhalts von Unterlagen auf Bildträger vom 31. Januar 1978 (StAnz. S. 472/475)
4. Gemeinsamer Runderlaß über die Verpflichtung zur Einhaltung des Datengeheimnisses nach § 9 HDSG vom 15. März 1978 (StAnz. S. 624)
5. Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen - auch für die automatisierte Verarbeitung gültig - vom 10. August 1978 (StAnz. S. 1706)
6. Erlaß über die Maßnahmen zur Durchführung des Hessischen Datenschutzgesetzes vom 10. Oktober 1978 (StAnz. S. 2011)

7. Erlaß zur Veröffentlichung gem. § 17 HDSG vom 5. Dezember 1978 (StAnz. S. 2539)

8. Mitteilungen von Bauvorhaben an Verlage für Bauten-Nachweise durch die unteren Bauaufsichtsbehörden vom 15. August 1979 (StAnz. S. 1800)

9. DV-Leitsätze (DVL)

   Arbeitsrichtlinien für die Automatisierung von Aufgaben der Landesverwaltung und der Kommunalverwaltung (Neufassung unter Berücksichtigung des HDSG) vom 9. Januar 1981 (StAnz. S. 395)

10. Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) vom 31. März 1981 (StAnz. S. 881)

11. Erlaß zur Übermittlung personenbezogener Daten an öffentliche Forschungseinrichtungen aus Dateien öffentlicher Stellen vom 13. Juni 1981 (StAnz. S. 1262).