



HESSISCHER LANDTAG

06. 02. 80

Achter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 5. Februar 1980 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag den folgenden Tätigkeitsbericht vor:

Eingegangen am 6. Februar 1980 · Ausgegeben am 10. Juli 1980

Druck: Carl Ritter & Co., Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 6200 Wiesbaden 1

INHALTSVERZEICHNIS

	Seite
1. Erster Teil	
Datenschutzprobleme – Schwerpunkte und Entwicklungstendenzen	5
1.1 Zur Situation	5
1.2 Bereichsspezifische Regelungen und mögliche Schwerpunkte	7
1.2.1 Sicherheitsbehörden	7
1.2.2 Personalausweis- und Melderechtsrahmengesetz	10
1.2.3 Sozialbehörden	10
1.2.4 Wissenschaftliche Forschung	11
1.2.5 Planungsdaten	12
1.2.6 Übermittlung an öffentlich-rechtliche Religionsgesellschaften	12
1.3 Organisatorische Maßnahmen	13
1.3.1 Auskunftsanspruch und Übermittlungssperre	13
1.3.2 Datensicherung und Löschung	14
1.3.3 Dezentralisierung der Verarbeitung	14
2. Zweiter Teil	
Datenschutzprobleme – Erfahrungen und Beispiele	16
2.1 Administrative und wissenschaftliche Befragungen	16
2.1.1 „Gasöldatei“/Abgabenordnung	16
2.1.2 Datenverarbeitung bei Beratungsstellen nach § 218 StGB	17
2.1.3 Sozialbericht bei Suchtkranken	17
2.1.4 Datenübermittlung bei Sozialstationen	19
2.1.5 Medizinisch-psychologische Untersuchungen	19
2.1.6 Übermittlung von Einwohnerdaten an Adreßbuchverlage	20
2.1.7 Wissenschaftliche Forschung und Datenschutz	21
2.1.8 Auftragsforschung	23
2.1.9 Fälle aus dem Bereich Forschung und Datenschutz	24
2.2 Transparenz der Datenverarbeitung	27
2.2.1 Erhebung von Daten beim Betroffenen	27
2.2.2 Dateienregister	27
2.2.3 Unterrichtung und Beratung über Datenschutzzusammenarbeit mit Datenschutz-Aufsichtsbehörden – Beteiligung an Lehrveranstaltungen	29
2.3 Entwicklung bei den Sicherheitsbehörden	30
2.3.1 Kriminalpolizeiliche Sammlungen (KpS)	30
2.3.2 Speicherung von Daten über Kinder in Polizeiinformationssystemen	31
2.3.3 Zur Auskunftsregelung bei Sicherheitsbehörden	33
2.3.4 Telefonische Auskunftersuchen der Polizei an Kraftfahrzeug-Zulassungsstellen und Einwohnermeldeämter	35
2.3.5 Bundeszentralregister und kriminalpolizeiliche personenbezogene Sammlungen	35
2.4 Datensicherung	36
2.4.1 Entwurf eines Maßnahmenkatalogs zur Datensicherung	36
2.4.2 Lösungsanspruch und Sicherungsdateien	38
2.4.3 Vernichtung von Datenträgern	40
2.4.4 DV-Entsorgungsspannen	41
2.4.5 Datenschutz und dezentralisierte Datenverarbeitung	43
2.4.6 Prüfungen bei den Rechenzentren des Hessischen Datenverarbeitungsverbundes	45
2.5 Praxis der Datenschutzkontrolle	46
2.5.1 Mitgliederverwaltung für Vereine durch KGRZ	46
2.5.2 Steuernummer	46
2.5.3 Neue Abrechnungsnachweise für Beamtengehälter	47

	Seite
2.6 Datenschutz im kirchlichen Bereich	47
2.6.1 Prüfungsvoraussetzungen	47
2.6.2 Der Datenschutz in der evangelischen Kirche in Hessen	48
2.6.3 Der Datenschutz in der katholischen Kirche in Hessen	49
2.6.4 Kirchliches Meldewesen	50
2.7 Bereichsspezifische Regelungen	51
2.7.1 Personalausweisgesetz	51
2.7.2 Melderechtsrahmengesetz	56
2.7.3 Änderung der Landeswahlordnung	57
2.7.4 Grenzüberschreitender Datenverkehr	58
a) Entwurf einer Konvention des Europarats	58
b) Entwurf von Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)	58
3. Dritter Teil	51
Materialien	51
3.1 Kirchliche Datenschutzbestimmungen	51
3.2 Vergleichende Übersicht über BDSG und KDO	69
3.3 „Datenschutz und Verwendung personenbezogener Angaben für Forschungszwecke“	83
– Grundsätze und Richtlinien, vorgelegt im Auftrag der European Science Foundation	

1. ERSTER TEIL

1. Erster Teil

Datenschutzprobleme — Schwerpunkte und Entwicklungstendenzen

1.1. Zur Situation

Fast zehn Jahre sind es mittlerweile her, seit der Hessische Landtag das erste Datenschutzgesetz verabschiedete. Die Entwicklung, die damit begann, wurde 1979 nahezu abgeschlossen: Die öffentliche Verwaltung ist, mit Ausnahme Hamburgs, bei der Verarbeitung personenbezogener Daten durchweg an eigens dafür formulierte, gesetzlich festgeschriebene Bedingungen gebunden. Zudem haben inzwischen die Datenschutzbeauftragten fast überall ihre Tätigkeit aufgenommen und darüber berichtet. Auch die Zahl der Bürger, die ihre in den Datenschutzgesetzen ausdrücklich anerkannten Rechte nicht nur kennenlernen, sondern auch selbst wahrnehmen wollen, ist beträchtlich gestiegen. Kurzum, die Bundesrepublik mag unstreitig zu den Ländern zählen, die im Rahmen ihrer Verwaltung die Verarbeitung personenbezogener Angaben konsequent automatisiert haben, sie ist aber zugleich das Land, in dem der Datenschutz wohl mit am deutlichsten greifbare Gestalt gewonnen hat.

Dennoch: 1979 ist nicht nur ein Jahr, in dem sich die Bereitschaft, den Datenschutz zu verwirklichen, bestätigt hat, sondern auch das Jahr, in dem die Zweifel am Erreichten und die Notwendigkeit, die bereits getroffenen Vorkehrungen zu verbessern, mindestens ebenso klar zum Ausdruck gekommen sind. Die lange und intensive Auseinandersetzung um den Personalausweis, die Bemühungen, das Melderecht neu zu formulieren, die Kritik am Sozialgeheimnis und die Forderung, es konkreter auszugestalten, sowie die Versuche, die Dateien der Sicherheitsbehörden den Anforderungen des Datenschutzes anzupassen, sind untrügliche Anzeichen dafür. Genauso symptomatisch ist freilich die erklärte Absicht aller politischen Parteien, das Bundesdatenschutzgesetz zu korrigieren.

Dem Bericht fällt unter diesen Umständen eine doppelte Aufgabe zu: Er muß wie immer Rechenschaft über die Tätigkeit des Datenschutzbeauftragten ablegen, zugleich jedoch die Schwerpunkte für künftige, im Interesse

des Bürgers unerläßliche Regelungen angeben. Er ist deshalb nicht nur Bilanz, sondern auch Forderungskatalog, konstatiert die Fortschritte und erinnert daran, daß der Datenschutz ein längst nicht abgeschlossener Prozeß ist, der den Gesetzgeber zu immer neuen Anstrengungen verpflichtet.

Einem recht verbreiteten Mißverständnis gilt es sofort zu begegnen: Die Aufgabe besteht keineswegs lediglich darin, die schon vorhandenen Datenschutzgesetze zu überprüfen und an dem einen oder anderen Punkt zu verbessern. Sicher fällt es nicht schwer, sowohl im öffentlichen als auch im nicht-öffentlichen Bereich Beispiele für die Notwendigkeit einer Korrektur auszumachen, angefangen bei der die Komplikationen förmlich provozierenden Anknüpfung an die Existenz einer Datei, über die höchst problematische Rolle der Einwilligung des Betroffenen in die Verarbeitung seiner Daten und die Nachteile der Verpflichtung, Gebühren für die Auskunft zu entrichten, bis hin zu den bedenklich geringen Kompetenzen der Aufsichtsbehörden. Doch die eigentliche und entscheidende Aufgabe liegt anderswo: Sie besteht in der Vorbereitung und Verabschiedung bereichsspezifischer Datenschutzregelungen. Nur in Kenntnis der konkreten Konflikte und der mit ihnen verbundenen Probleme kann es wirklich gelingen, die allgemein gehaltenen Formulierungen der Datenschutzgesetze durch präzise, den Schutz des Bürgers tatsächlich garantierende Verhaltensanweisungen abzulösen. Erst unter dieser Voraussetzung lassen sich beispielsweise die Grenzen der Auskunftsverpflichtung ebenso überzeugend ziehen, wie die Schranken der Speicherung und Übermittlung in einer Weise umschreiben, die der Betroffene nachvollziehen und deshalb letztlich auch kontrollieren kann.

Sowohl der Hinweis auf festgestellte Datenschutzdefizite als auch der Versuch, Schwerpunkte der weiteren Aktivität des Gesetzgebers zu beschreiben, sind deshalb zuvörderst Material für eine Datenschutzregelung, die sich bewußt und gezielt von der Abstraktion der Datenschutzgesetze abwendet und der gezielten Reaktion auf bestimmte kritische Fallkonstellationen den Vorzug gibt. So notwendig die Korrektur der Datenschutzgesetze

deshalb sein mag, sie ersetzt nicht, sondern ergänzt bestenfalls die Verpflichtung zur bereichsspezifischen Regelung.

Die Fähigkeit des Datenschutzbeauftragten, Regelungsschwerpunkte anzugeben und damit Parlament und Regierung auf die im Interesse des Bürgers notwendigen Interventionen aufmerksam zu machen, hängt freilich entscheidend von der Möglichkeit ab, seine vom Datenschutzgesetz vorgeschriebene Kontrollaufgabe uneingeschränkt wahrzunehmen. Erst wenn er tatsächlich in der Lage ist, den Verarbeitungsprozeß offenzulegen und jedem seiner Aspekte nachzugehen, kann er die Tragweite der vorhandenen und die Ansatzpunkte weiterer Datenschutzregelungen abschätzen. Der Datenschutzbeauftragte ist insofern bei seiner Tätigkeit in hohem Maße auf die Bereitschaft der Exekutive zur Kooperation angewiesen. Die Landesregierung hat diese Bereitschaft im Berichtszeitraum vor allem durch einen Kabinettsbeschluß vom 23. Oktober 1979 zum Ausdruck gebracht, der über die Grenzen Hessens hinaus Beachtung verdient. Er sieht vor, daß bei datenschutzrelevanten Fragen der Datenschutzbeauftragte vor jeder Entscheidung eingeschaltet werden muß. Er erhält damit die Möglichkeit, sich rechtzeitig zu äußern und auf notwendige Schutzvorkehrungen zu einem Zeitpunkt aufmerksam zu machen, zu dem sie leichter und wirksamer zu verwirklichen sind. Mehr denn je wird damit zugleich anerkannt, daß der Datenschutz ein unverzichtbarer Bestandteil rechtsstaatlicher Verwaltung ist, die Auseinandersetzung mit seinen Anforderungen also zu den selbstverständlichen Grundbedingungen administrativer Aktivität gehört.

Die Bereitschaft der Landesregierung zur Zusammenarbeit kommt genauso in einer Reihe rechtspolitischer Initiativen zum Ausdruck. Das gilt in erster Linie für die Reform des Personalausweisrechts. Hier hat die Landesregierung auf dem Hintergrund der Kooperation mit dem Datenschutzbeauftragten dem Bundesrat Vorschläge unterbreitet, die entscheidend zur Korrektur der ursprünglich geplanten Regelung beigetragen haben. Das gilt aber auch für die noch ausstehende Reform des Hessischen Krankenhausgesetzes. Einmal mehr geht es darum, konkrete Erfahrungen in eine Regelung umzumünzen, die dem Schutz der persönlichen Integrität des Bürgers Rechnung trägt. Landesregierung und Datenschutzbeauftragter versuchen, den im Interesse des Bürgers bestmöglichen Weg gemeinsam auszumachen, die mit der Verar-

beitung medizinischer Daten verbundene Gefährdung also von vornherein auszuschalten. Das gilt schließlich für die nunmehr von der Landesregierung akzeptierte Notwendigkeit, auf Gebühren für die Erteilung von Auskünften nach dem Datenschutzgesetz zu verzichten. Die Bedenken gegen die Gebührenpflicht waren schon im Rahmen der parlamentarischen Diskussion über das zweite Hessische Datenschutzgesetz geäußert worden. Die Landesregierung hatte seinerzeit gemeint, sich der vom Bundesgesetzgeber eingenommenen Haltung anschließen zu müssen. Sie hat sich aber nicht der Kritik und den Vorschlägen des Datenschutzbeauftragten verschlossen und folgt nunmehr mit ihrem Entwurf der im Sechsten Tätigkeitsbericht befürworteten Regelung. Sie knüpft damit zugleich an die in der Vergangenheit immer wieder bekundete Bereitschaft des Landes Hessen an, den Datenschutz kontinuierlich zu verbessern, und zwar selbst dann, wenn die in Hessen angestrebten Maßnahmen von den anderswo akzeptierten Vorschriften abweichen.

So begrüßenswert und wichtig diese Zusammenarbeit ist, so wenig darf sie über die Schwierigkeiten hinwegtäuschen, die nach wie vor bei der gesetzlich vorgeschriebenen Kontrolle der Verarbeitung personenbezogener Daten im Rahmen der öffentlichen Verwaltung bestehen. Das Datenschutzgesetz verzichtet bewußt auf Ausnahmen. Die Überwachung erstreckt sich nicht auf einzelne, unter welchen Gesichtspunkten auch immer ausgewählte Bereiche der öffentlichen Verwaltung, sie erfaßt die gesamte staatliche Aktivität. Damit sind die Versuche der Steuerverwaltung nicht zu vereinbaren, die Kontrollbefugnisse des Datenschutzbeauftragten einzuschränken. Sie lassen sich auch nicht mit dem wiederholten Hinweis auf die Bedeutung des Steuergeheimnisses begründen. Der Gesetzgeber hat mit § 30 der Abgabenordnung unstreitig eine Vorschrift geschaffen, die dem Schutz des Betroffenen dient und sich insoweit ihrer ganzen Zielsetzung nach mit den Regeln des Datenschutzgesetzes vergleichen läßt. Gerade deshalb zählt § 45 BDSG den § 30 AO zu den Bestimmungen, die dem Bundesdatenschutzgesetz vorgehen. Nur ist damit nicht mehr als die materielle Regelung gemeint. Der Datenschutz soll sich mit anderen Worten nach den besonderen, in der Abgabenordnung näher definierten Voraussetzungen richten. Mit ihnen ist aber noch nichts über die auch im Bereich der Steuerverwaltung im Interesse des Betroffenen unerläßliche Kontrolle der Ver-

arbeitung gesagt. Nicht von ungefähr weist das Hessische Datenschutzgesetz (§ 23 Abs. 1) genauso wie alle übrigen Datenschutzgesetze dem Datenschutzbeauftragten die Aufgabe zu, nicht nur die Einhaltung des HDSG zu überwachen, sondern auch aller anderen von der öffentlichen Verwaltung zu beachtenden Datenschutzvorschriften. Das Gesetz schreibt um des Bürgers willen eine Kontrolle vor, die sich eben nicht nach dem Zufall richtet, wo jeweils eine Datenschutzbestimmung vorkommt. Vielmehr ist es eine der wichtigsten Funktionen des Datenschutzbeauftragten, ohne Rücksicht auf die einzelgesetzliche Grundlage für einen wirksamen Datenschutz im Gesamtbereich der öffentlichen Verwaltung zu sorgen.

Jeder Versuch, davon abzugehen, stellt die vom Gesetzgeber gewollte und in den Datenschutzgesetzen ausdrücklich akzeptierte Kontrolle in Frage. Ein „Geheimnis“ gibt es schließlich nicht nur im Bereich der Finanzverwaltung. Genauso nahe läge es, auf § 35 SGB I und das Sozialgeheimnis zu verweisen – um nur dieses eine Beispiel zu nennen – und damit die Sozialbehörden aus der Überwachung durch den Datenschutzbeauftragten auszunehmen. Und wer sich im öffentlichen Bereich zu einer solchen Interpretation bereifindet, muß über kurz oder lang ähnliche Schlußfolgerungen für den nicht-öffentlichen ziehen. Der Hinweis auf die ärztliche Schweigepflicht drängt sich von selbst auf, mit der Konsequenz, daß die Kontrollaufgabe der Aufsichtsbehörde nicht minder wirksam beschnitten würde. Noch einmal aber: Landes- und Bundesgesetzgeber haben in der konsequenten und kontinuierlichen Überwachung mit die wichtigste Voraussetzung des Datenschutzes gesehen. Sie begnügen sich daher keineswegs damit, bestimmte Anforderungen an den Verarbeitungsprozeß zu stellen, sondern entscheiden sich zugleich für eine besondere, eigens dafür geschaffene Instanz, die keinen anderen Sinn hat, als durch die Überwachung der Datenschutzvorschriften dem Bürger die Gewißheit zu vermitteln, daß diese Regeln nicht nur ein bloßer Appell an die öffentliche Verwaltung sind, sondern tagtäglich praktizierter Bestandteil ihres Verhaltens. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder den Versuch der Finanzverwaltung, sich zumindest teilweise der Kontrolle zu entziehen, entschieden zurückgewiesen. Und aus dem gleichen Grund gilt es, sich zu vergegenwärtigen, daß es hier um mehr geht, als nur um Sonderprobleme eines bestimmten Bereichs der öffentlichen

Verwaltung. Jede Restriktion der Kontrollbefugnisse des Datenschutzbeauftragten leitet eine Entwicklung ein, die in offenem Widerspruch zu dem in der Datenschutzgesetzgebung verbürgten Schutz des Bürgers gegen die sich aus der Verarbeitung seiner Daten ergebenden Gefahren steht.

1.2. Bereichsspezifische Regelungen und mögliche Schwerpunkte

1.2.1 Sicherheitsbehörden

Fragt man nun nach den Defiziten der vorhandenen und den Schwerpunkten einer neuen und besseren Regelung, dann spricht viel dafür, mit einigen Bemerkungen zum Sicherheitsbereich zu beginnen. Hier hat die Kritik schon sehr früh eingesetzt: Den Datenschutzgesetzen genügt durchweg der bloße Hinweis auf die „öffentliche Sicherheit oder Ordnung“, um das ansonsten für selbstverständlich gehaltene Auskunftsrecht des Betroffenen zu verweigern. Zudem hat sich spätestens an der Diskussion über das Melderecht und über die Dateien der Sicherheitsbehörden gezeigt, wie sehr es im Interesse der Bürger darauf ankommt, präzise Übermittlungsregeln zu entwickeln. Und schließlich spielt gerade hier die Forderung nach einem kontrollierten Vergessen eine besonders wichtige Rolle. Insofern überrascht es nicht, wenn der Sicherheitsbereich gleichsam zum Musterbeispiel für die Notwendigkeit bereichsspezifischer Regelungen wird.

Jeder Schritt in diese Richtung setzt allerdings die Bereitschaft voraus, auf den bislang verwendeten allgemeinen Hinweis auf den Sicherheitsbereich endgültig zu verzichten. Statt dessen gilt es, sich unmittelbar an den einzelnen Sicherheitsbehörden und ihren Aufgaben zu orientieren. Der gemeinsame Nenner „öffentliche Sicherheit“ ändert nichts an der besonderen Aufgabenstellung jeder dieser Behörden und deshalb an der Notwendigkeit, Voraussetzung und Grenzen der Verarbeitung personenbezogener Daten in Kenntnis der einzelnen Funktionen zu bestimmen. Ebenso wenig wie es anderswo angeht, von der jeweiligen Aufgabe abzusehen, rechtfertigen sich hier Regeln, die nicht strikt aufgabenbezogen sind. Der Datenschutz duldet keine Blanko-, sondern nur eine funktionsbezogene Ermächtigung zur Verarbeitung. Jeder gesetzlichen Vorschrift, die zur Verarbeitung berechtigt, muß daher eine Regelung vorausgehen, die den Aufgabenbereich der Behörden offenlegt und festschreibt.

Nur unter dieser Voraussetzung kann es gelingen, die gegenwärtige Auskunftregelung durch Bestimmungen zu ersetzen, die den Datenschutzerfordernissen wirklich entsprechen. Sicher, bereits bisher läßt es das Gesetz nicht bei der mit dem Hinweis auf die öffentliche Sicherheit verbundenen Informationssperre (§ 18 Abs. 3 Nr. 2). Der Bürger hat die Möglichkeit, sich an den Datenschutzbeauftragten zu wenden und ihn zu veranlassen, festzustellen, ob sich die Verarbeitung an die gesetzlichen Voraussetzungen hält. Und in der Tat machen immer mehr Bürger von dieser Möglichkeit Gebrauch. Das Ergebnis ist freilich nicht gerade dazu geeignet, sie vom Datenschutz zu überzeugen. Der Datenschutzbeauftragte kommt zwar seiner Aufgabe nach, und auch die Sicherheitsbehörden sind in aller Regel durchaus bereit, sich der Kontrolle zu unterziehen. Der Nachteil des Verfahrens wird jedoch dann sichtbar, wenn es darum geht, den Betroffenen zu unterrichten. Was den Sicherheitsbehörden untersagt ist, muß der Datenschutzbeauftragte ebenfalls respektieren. Die „öffentliche Sicherheit“ verbietet es ihm, über Art und Inhalt der Verarbeitung Auskunft zu geben. Mehr, als daß die gesetzlichen Vorschriften beachtet worden sind, kann er nicht sagen. Für den Betroffenen ist damit kaum etwas gewonnen. Ob er registriert ist oder nicht, bleibt ihm verborgen. Aus seiner Perspektive stellt sich insofern der Hinweis auf die Einhaltung des Gesetzes als ein reichlich merkwürdiges Spiel mit seiner Ungewißheit dar.

Ganz abgesehen davon nährt die stets gleichlautende, ständig wiederkehrende Auskunftsverweigerung den Verdacht, daß die Feststellung, der Datenschutz kenne auch und gerade im behördlichen Bereich keine Ausnahme, dort nicht mehr gilt, wo die Gefahren für den Bürger am handgreiflichsten zu sein scheinen. Die Konsequenz: Der Gesetzgeber diskreditiert sich und die Sicherheitsbehörden. Je weniger der Gesetzgeber deshalb unternimmt, um diesen Eindruck zu zerstreuen, desto mehr stigmatisiert er die betroffenen Behörden und drängt deren Bedienstete in eine Außenseiterrolle.

Deshalb geht es nicht an, eine Regelung weiter hinzunehmen, die im Verhältnis zum Bürger Sprachlosigkeit und nicht Kommunikation zur Folge hat und im Verhältnis zu den Sicherheitsbehörden die Meinung bestärkt, das Gesetz billige, ja strebe eine Sonderbehandlung an. Kurzum, was ansonsten die Regel ist, muß hier genauso gelten: Die Auskunft ist die

Kehrseite der Verarbeitung. Der Bürger muß die Verwendung seiner Daten nur solange hinnehmen, wie er auch die Möglichkeit hat, sich selbst zu vergewissern, was mit diesen Angaben geschieht. Der Begründung bedarf infolgedessen nicht die Erteilung, sondern immer nur die Verweigerung der Auskunft. Sie kann jedoch nur den Anforderungen des Datenschutzes genügen, wenn Vorkehrungen formuliert werden, die konkret an die spezifische Aufgabe der Behörde und den Zweck der einzelnen Datei anknüpfen. Erst dort, wo beides feststeht, läßt sich wirklich sagen, ob und in welchem Umfang der Auskunftspflicht Grenzen gezogen werden müssen, zugleich aber dem Betroffenen verständlich machen, um welchen Sachverhalt es geht und warum dessen Besonderheiten dazu zwingen, vom generellen Grundsatz abzuweichen. Konsequenter wahrgenommener Datenschutz verlangt daher den Verzicht auf die bisher praktizierte Regelungstechnik und eine detaillierte Auseinandersetzung mit den Verarbeitungsmodalitäten anhand der einzelnen Dateien und in Kenntnis der jeweiligen Behördenfunktionen (siehe auch: 2.3.3).

Damit läßt sich freilich weit mehr erreichen, als nur eine datenschutzkonforme Formulierung des Auskunftsrechts. Genauso betroffen ist die Verpflichtung der Sicherheitsbehörden, die Verarbeitung an feste zeitliche Grenzen zu binden. Die Speicherung läßt sich nur so lange rechtfertigen, wie auch Gewißheit über den Zeitraum besteht, innerhalb dessen auf die Daten zurückgegriffen werden darf. Nicht von ungefähr widersetzt sich der Gesetzgeber in § 49 BZRG jedem Versuch, den Betroffenen immer wieder mit seiner Vergangenheit zu konfrontieren. Zu den Aufgaben des Datenschutzes gehört es auch, die Chance des Betroffenen sicherzustellen, nicht ständig von der eigenen Vergangenheit eingeholt zu werden. Nur hat sich, nicht zuletzt im Zusammenhang mit meinem letzten Tätigkeitsbericht, gezeigt, wie umstritten die Anwendungsgrenzen des § 49 BZRG sind. Die Feststellung, daß nach Eintritt der Tilgungsreife eine Weitergabe innerhalb der Polizei nach wie vor zulässig ist, weil die Daten nicht im Rechtsverkehr zum Nachteil des Betroffenen verwertet werden, sondern lediglich um den Sachverhalt aufzuklären, vermag freilich nicht zu überzeugen. Solche Unterscheidungen stellen die Glaubwürdigkeit der im BZRG vom Gesetzgeber getroffenen Entscheidung in Frage. Sie verträgt sich nicht mit einem wie auch immer begründeten System von Parallel- und Nebenakten. Der Zeitablauf muß eine

generell verbindliche Verarbeitungsschranke sein, soll der Betroffene wirklich nicht immer wieder nach seinem früheren Verhalten beurteilt werden. Wenn man aber trotzdem meint, von der Regelung des BZRG abweichen zu müssen, kann und darf es nur gesetzlich abgesicherte, sorgfältig eingeschränkte und durch ihre Regelung restlos offengelegte Ausnahmen geben (siehe auch: 2.3.5).

Wie wenig es angeht, sich mit abstrakten und letztlich nichtssagenden Aussagen abzufinden, zeigt sich am Beispiel der Registrierung von strafunmündigen Kindern. Sicher ist die Polizei mit Rücksicht auf ihre Verpflichtung, der Kriminalität vorzubeugen, auch an Informationen über das Verhalten von Strafunmündigen interessiert. Nur: Kinder in polizeiliche Informationssysteme aufzunehmen oder sonst zu registrieren, heißt die vom Gesetzgeber garantierte Strafunmündigkeit umgehen. Das unter strafrechtlichen Gesichtspunkten eben nicht zur Kenntnis genommene Verhalten wird auf dem Umweg über die Verarbeitung zu einer für die Beurteilung des Betroffenen relevanten Information: Insofern steht hier keineswegs nur die Lösungsfrist auf dem Spiel, sondern die Zulässigkeit der Speicherung. Wenn eine Verarbeitung überhaupt in Betracht gezogen werden muß, so grundsätzlich nur bei den Behörden und Stellen, die ihrer ganzen Aufgabe nach Hilfestellung bei der Entwicklung der Kinder zu leisten haben und ausschließlich unter diesem Gesichtspunkt. Kriminalpolitische Erkenntnisse lassen sich auch auf anderem Weg als über die Verarbeitung individueller Daten erzielen (siehe auch: 2.3.2).

Die mit dem Datenschutz untrennbar verbundene Verpflichtung zu einem programmierten Vergessen hat nicht zuletzt im Zusammenhang mit dem Versuch, Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen auszuarbeiten, eine wichtige Rolle gespielt. Was im letzten Tätigkeitsbericht ausdrücklich gesagt worden ist, gilt nach wie vor: Die Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) sind aus der Perspektive des Datenschutzes ein bedeutsamer Beitrag zur Verbesserung der Position des Bürgers. Dies ist in der Zwischenzeit auch von den Datenschutzbeauftragten der Länder und des Bundes bejaht worden. Deshalb stimmt es bedenklich, wenn die bereits vorliegenden Richtlinien nicht in Kraft gesetzt worden sind. Sicherlich sind Verbesserungen erforderlich. Sie recht fertigen es aber nicht, Vorschriften, die einen

erheblichen Fortschritt darstellen, nicht zu praktizieren. Die Aufgabe kann vielmehr nur darin bestehen, die einmal akzeptierten Regeln weiterzuentwickeln und damit immer mehr einem konsequenten Datenschutz anzupassen.

Die KpS-Richtlinien sind um so wichtiger, als mit ihrer Hilfe durchaus verdeutlicht werden kann, wie sich die vom Datenschutz geforderte Verrechtlichung des Informationsverhaltens der Sicherheitsbehörden verwirklichen läßt. Fest steht zunächst soviel: Einen regelungsfreien Raum darf es nicht geben. Dem Gesetzgeber fällt unter allen Umständen die Aufgabe zu, die Funktionen der einzelnen Behörden ebenso festzulegen wie ihre Berechtigung, Dateien im Hinblick auf ihre gesetzlich fixierten Aufgaben einzurichten. Daneben ist es durchaus denkbar und zulässig, auf Rechtsverordnungen und Verwaltungsvorschriften in Gestalt von Richtlinien zurückzugreifen. Gerade mit Hilfe der Richtlinien läßt sich die Verarbeitung den jeweiligen Aufgaben anpassen. Nur sind sie lediglich so lange tragbar, wie sie in Kenntnis und unter genauer Berücksichtigung des Datenschutzes entstehen und auch veröffentlicht werden. Die Flexibilität darf nicht auf Kosten des Schutzes des Bürgers gehen. Dieser hängt aber entscheidend von der Transparenz der für die Behörden geltenden Verhaltensregeln ab. Die Erfahrung zeigt jedoch, daß die Offenlegung mit dem Übergang zu Verwaltungsvorschriften abnimmt. Hier gilt es deshalb rechtzeitig Vorkehrungen zu treffen, die eine Transparenz sicherstellen.

Und noch ein weiteres: Richtlinien sind nicht zuletzt ein Mittel, um Erfahrungen bei der Verwirklichung des Datenschutzes zu sammeln. Ihre Anpassungsfähigkeit beinhaltet insofern auch die Möglichkeit, festgestellte Mängel möglichst schnell und wirksam zu beheben. Eine Überlegung, die um so schwerer wiegt, als sich der Datenschutz für alle Beteiligten nach wie vor als Lernprozeß darstellt. Nur, so wichtig Richtlinien gegenwärtig sind, sie dürfen zumindest in ihrem augenblicklichen Umfang nicht als Instrument einer Dauerregelung gesehen und verstanden werden. Der Gesetzgeber muß vielmehr die mit ihrer Hilfe gewonnenen Erfahrungen nutzen, um sie soweit wie möglich durch gesetzliche Regelungen abzulösen. Die Richtlinien sind insofern unvermeidliche Zwischenstationen auf dem Weg zu gesetzlichen Vorschriften und deshalb ein Provisorium. Regierung und Gesetzgeber sind daher verpflichtet,

die Verwendung von Richtlinien fortwährend zu überprüfen und fortschreitend zu reduzieren. Die Variabilität der Regelungsinstrumente stellt mit anderen Worten nicht die Priorität des Gesetzes in Frage. Wo davon abgewichen wird, bedarf es der besonderen Rechtfertigung und der Anbindung an Vorkehrungen, die einer Verminderung des Datenschutzes entgegenwirken (siehe auch: 2.3.1).

1.2.2 Personalausweis- und Melderechtsrahmengesetz

Personalausweis- und Melderechtsrahmengesetz sind die wohl bezeichnendsten Beispiele für eine bereichsspezifische Datenschutzregelung. Bei beiden ist die Diskussion lange ohne Berücksichtigung der Datenschutzerfordernungen geführt worden. Bei beiden ist gerade im vergangenen Jahr ein bemerkenswerter Wandel festzustellen. Das mittlerweile verabschiedete Personalausweisgesetz enthält jetzt eine ganze Reihe von Vorkehrungen, die im Interesse des Bürgers konzipiert und formuliert worden sind. Das gilt für die strikte gesetzliche Beschränkung der in den Personalausweis aufgenommenen Angaben ebenso wie für die nunmehr garantierte Lesbarkeit durch den Betroffenen und die Zurückweisung aller Versuche, das Personenkennzeichen doch noch auf dem Umweg über den Personalausweis einzuführen. Auch der Entwurf des Melderechtsrahmengesetzes nimmt von den bisher maßgeblichen Vorstellungen Abstand. Er versucht statt dessen, ganz im Sinne einer strikt bereichsspezifischen Regelung, die Aufgabe der Meldebehörden zu definieren und die Verarbeitungsbedingungen daran zu orientieren. Zum ersten Mal liegt insofern im Meldebereich ein Gesetzesvorschlag vor, der nicht am Datenschutz vorbei, sondern im Bestreben, seinen Anforderungen zu genügen, formuliert worden ist. Nur wäre es falsch zu meinen, die Diskussion sei damit beendet. Im Gegenteil, sie ist an einem besonders kritischen Punkt angelangt. Der Gesetzgeber hat mit den im Personalausweisgesetz getroffenen Vorkehrungen die Befürchtungen zu zerstreuen versucht, die im Hinblick auf die Maschinenlesbarkeit des Ausweises geäußert worden sind. Nur: die im Personalausweisgesetz enthaltene Regelung ist solange letztlich wirkungslos, wie sie nicht durch entsprechende Vorschriften im Melderecht ergänzt wird. Übermittlungsverbote nützen mit anderen Worten dann nichts, wenn sie über allgemeine Übermittlungsvorschriften, wie sie sich etwa in § 18 des Melderechtsrahmengesetzentwur-

fes finden, jederzeit und ohne Schwierigkeiten umgangen werden können. Die Gefahr für den Bürger liegt in der zeitlich verschobenen Verabschiedung von Gesetzen, die sich in Wirklichkeit nicht voneinander trennen lassen. Unter Datenschutzgesichtspunkten sind Personalausweis-, Melderechtsrahmengesetz und die Bestimmungen über die Verarbeitung personenbezogener Angaben in den verschiedenen Dateien der Sicherheitsbehörden unauflöslich miteinander verbunden. Keine dieser Maßnahmen läßt sich isoliert betrachten; erst zusammengenommen schaffen sie die Grundlage für einen verlässlichen Datenschutz, eine Feststellung, die durch den Beschluß des Bundestages vom 17. Januar 1980 (zu BR-Drucks. 17/80) bekräftigt wurde.

Deshalb ist die positive Beurteilung des Personalausweisgesetzes an die Bedingung geknüpft, daß Gesetzgeber und Regierung auch in den beiden anderen Fällen nach genau den Maximen handeln, die sie im Personalausweisgesetz akzeptiert haben. Ein Melderecht, das Übermittlungsvorschriften in ihrer gegenwärtig geplanten Fassung enthält, zwingt insofern dazu, die Korrektur des Personalausweisgesetzes zu fordern. Und genau der gleiche Vorbehalt muß so lange bestehen bleiben, wie nicht Klarheit über die Dateien der Sicherheitsbehörden und die für sie geltenden Vorschriften besteht.

Besondere Aufmerksamkeit verdient auch das von der Bundesdruckerei bei der Herstellung der Ausweise anzuwendende Verfahren. Scheinbar unüberwindliche technische Schwierigkeiten dürfen nicht zum Anlaß genommen werden, um die restriktiven Bestimmungen des Personalausweisgesetzes in Frage zu stellen. Das Herstellungsverfahren hat sich nach den im Gesetz festgeschriebenen Prioritäten zu richten. Die Verpflichtung, sich anzupassen, trifft infolgedessen in vollem Umfang das Herstellungsverfahren und nicht das Gesetz. Einmal mehr erweist sich aber daran, wie sehr es darauf ankommt, sich nicht mit dem Gesetzestext zufriedenzugeben, sondern auch alle damit zusammenhängenden Ausführungsvorschriften genauso streng unter Datenschutzgesichtspunkten zu prüfen (siehe auch: 2.7.1, 2.7.2).

1.2.3 Sozialbehörden

Folgt man einem in der Öffentlichkeit weit verbreiteten Eindruck, dann reduziert sich die Frage nach der Existenz und der Wirksamkeit von Datenschutzevorkehrungen mehr oder

weniger auf die Kontrolle der Verarbeitung personenbezogener Angaben durch die Sicherheitsbehörden. Die Erfahrung der Datenschutzbeauftragten legt freilich einen ganz anderen Schluß nahe. So verständlich das Interesse am Sicherheitsbereich ist, so wenig darf darüber übersehen werden, daß die Notwendigkeit einer Regelung sich nirgends so aufdrängt wie im Sozialbereich. Hier macht sich die Konsequenz der gewandelten Aufgabenstellung der öffentlichen Verwaltung, ihrer Verpflichtung, in immer größerem Umfang Leistungen an den Bürger zu erbringen, unmittelbar bemerkbar: die ständig zunehmende Verarbeitung der unterschiedlichsten Angaben von schlichten „Alltagsdaten“, wie etwa dem Namen oder der Adresse bis hin zu überaus sensiblen Informationen über die Gesundheit des Betroffenen. Hier ist es deshalb für den Bürger von ganz entscheidender Bedeutung, daß rechtzeitig Vorkehrungen entwickelt werden, die jeder Zweckentfremdung seiner Daten rechtzeitig vorbeugen, die Sozialverwaltung also nicht zu einem für die verschiedensten Ziele verwendbaren Datenfundus der öffentlichen Verwaltung werden lassen.

Gewiß, eine erste Reaktion des Gesetzgebers liegt vor. Das in § 35 SGB I anerkannte Sozialgeheimnis ist eine ebenso notwendige wie elementare Datenschutzvorkehrung. Doch das Sozialgesetzbuch liefert mit seiner Vorschrift nicht mehr als den Ansatzpunkt für längst fällige bereichsspezifische Regelungen. Der Sozialbericht bei Suchtkranken ist dafür ebenso bezeichnend wie die Datenübermittlung bei Sozialstationen. Im einen wie im anderen Fall geht es um die Verwendung der Daten des Betroffenen in einem Zusammenhang, der nicht mehr seine persönliche Situation zum Gegenstand hat, sondern die Wirtschaftlichkeit der jeweils getroffenen Maßnahmen und die Rechnungslegung darüber. Der Anspruch der Verwaltung mag seinen guten Sinn haben, er kollidiert aber mit der vom Datenschutz gedeckten Erwartung des Betroffenen, daß die Verwendung seiner Angaben grundsätzlich nur zu Zwecken geschehen darf, die ihm bekannt sind und die er auch überblicken kann. Je mehr er sich aber gerade mit Rücksicht auf die ihm angebotene Hilfe bereitfindet, Angaben zu seiner Person offenzulegen, desto strenger müssen die Maßstäbe sein, nach denen Einsicht in diese Angaben zu anderen als den ursprünglichen Zwecken genommen werden kann.

Unzweifelhaft sind Sozialbehörden Teil der öffentlichen Verwaltung, und ebensowenig

läßt sich die Verpflichtung bestreiten, genauso wie jede andere öffentliche Stelle Rechenschaft über die verwendeten öffentlichen Mittel abzulegen. Dennoch darf deshalb der Datenschutz nicht in Frage gestellt werden. Vielmehr gilt es, Verfahren zu entwickeln, die einen Zugriff auf die personenbezogenen Angaben soweit wie möglich ausschließen. Die Datenschutzgesetze legen Prioritäten fest, die von der öffentlichen Verwaltung zu beachten sind. Die Konsequenz kann unter diesen Umständen nur eine strenge Abschottung der Sozialbehörden und die Entwicklung von Übermittlungsvorschriften sein, die auf die spezifische Aufgabe eben dieser Behörden Rücksicht nehmen. Das Sozialgeheimnis genügt dafür nicht. Es läßt weder die Grenzen der Amtshilfe verlässlich erkennen noch sind ihm Verfahren zu entnehmen, die den Schutz des Betroffenen eindeutig sicherstellen. Die Formulierung des § 35 SGB I ist viel zu allgemein gehalten, um die für solche Verfahren erforderlichen präzisen Verhaltensregeln erkennen zu können. Den Ausweg bieten nur Vorschriften, die von den konkreten Aufgaben der Sozialbehörden ausgehen und deshalb auch in der Lage sind, die Verarbeitungsvoraussetzungen und vor allem die Übermittlungsgrenzen mit Rücksicht auf die jeweils erhobenen Daten und ihre Bedeutung für den Betroffenen zu definieren (siehe auch: 2.1.3, 2.1.4).

1.2.4 Wissenschaftliche Forschung

Verständlicherweise haben bereits in der Vergangenheit die vor allem in Schulen für Zwecke der wissenschaftlichen Forschung verteilten Fragebögen Kritik und Mißtrauen hervorgerufen. Sie sind in aller Regel nicht nur sehr detailliert, sondern dem Betroffenen kaum verständlich. Mit jedem neuen Fragebogen aktualisiert sich freilich eine der größten Schwierigkeiten, vor die sich jeder Versuch gestellt sieht, den Datenschutz so wirksam wie nur möglich auszugestalten. Der Gesetzgeber hat zwar unmißverständlich zu erkennen gegeben, daß jede Verarbeitung personenbezogener Angaben an die gesetzlich vorgeschriebenen Verarbeitungsbedingungen gebunden ist. Wer die Daten haben möchte, ist insofern gleichgültig. Den Ausschlag gibt allein die Intention, personenbezogene Angaben zu verarbeiten. Nur: Auch die gesetzliche Regelung des Datenschutzes kann nicht umhin, die in der Verfassung garantierte Freiheit der wissenschaftlichen Forschung zu respektieren. Der Gesetzgeber muß infolge-

dessen für Bestimmungen sorgen, die Forschung ermöglichen, ohne die persönliche Integrität derjenigen zu gefährden, deren Daten verarbeitet werden sollen.

Das Hessische Datenschutzgesetz hat versucht, dieser Forderung in § 15 Rechnung zu tragen. Andere Landesgesetze haben den dort eingeschlagenen Weg ebenfalls befolgt. Hinzu kommt eine Reihe auf wissenschaftliche Untersuchungen gemünzter Bestimmungen, die vom Hessischen Kultusminister in Zusammenarbeit mit dem Datenschutzbeauftragten ausgearbeitet worden sind. Dennoch ist die Situation alles andere als zufriedenstellend. Zunächst: Hessen ist zwar dasjenige Bundesland, das über die detaillierteste Regelung verfügt. Nur ist die Diskrepanz zwischen den rechtlichen Anforderungen und der Erhebungspraxis offenkundig. Die im Interesse eines wirksamen Datenschutzes formulierten Bestimmungen bleiben weitgehend unbeachtet.

Ganz abgesehen davon ist es jedoch an der Zeit, sich nicht mehr mit § 15 zu begnügen, sondern eine in sich geschlossene, sich auf die bisherigen Erfahrungen gründende bereichsspezifische Regelung vorzulegen. Nur unter dieser Voraussetzung kann es gelingen, sowohl die Bedingungen klarzustellen, unter denen die etwa für Stichproben erforderlichen Daten zur Verfügung gestellt werden müssen, als auch die Grenzen der zeitlichen Aufbewahrung der verarbeiteten Daten, um nur diese beiden immer wieder zur Debatte stehenden Fragen zu nennen. Die European Science Foundation hat Richtlinien für eine solche Regelung vorgelegt. Anders als sonst wird hier die Notwendigkeit des Datenschutzes auch und gerade im Zusammenhang mit wissenschaftlichen Untersuchungen nicht geleugnet, sondern ausdrücklich akzeptiert. Die Vorschläge sind insofern ein gezielter Versuch, praktikable Verhaltensanweisungen zu formulieren. Sie eignen sich daher durchaus als Anhaltspunkt für eine Regelung, die über den § 15 hinausführt. Solange sie nicht vorliegt, wird weder das Mißtrauen gegenüber wissenschaftlichen Untersuchungen abgebaut, noch der Verdacht, der Datenschutz entwickle sich mehr und mehr zum Hindernis wissenschaftlicher Forschung, zerstreut werden können. Es liegt daher sowohl im Interesse der Betroffenen als auch der wissenschaftlichen Forschung, nicht weiter abzuwarten. Noch einmal freilich: Eine Priorität der wissenschaftlichen Forschung gegenüber dem vom Gesetzgeber anerkannten Schutz der persön-

lichen Integrität gibt es nicht. Umgekehrt darf aber auch der Datenschutz nicht zum Vorwand genommen werden, um Forschungsaufgaben und Forschungstätigkeit zu gefährden. Den Ausgleich zu finden, ist sicherlich nicht leicht, nur kann und darf deshalb der Versuch, es zu tun, nicht immer weiter hinausgeschoben werden (siehe auch: 2.1.7 – 2.1.9, 3.3).

1.2.5 Planungsdaten

Die Diskussion über die Novellierung der Statistikgesetze hat erneut die Notwendigkeit einer besonderen Bestimmung über die Verarbeitung personenbezogener Angaben zu Planungszwecken unterstrichen. Der Datenschutz zwingt dazu, sich zunächst streng an den Zweck der Erhebung und Speicherung zu halten. Umgekehrt läßt sich der Bedarf an personenbezogenen Daten auch und gerade im Zusammenhang mit den für den Bürger wichtigen Entwicklungsvorhaben von Staat und Kommunen nicht übersehen. Eine Übermittlung muß aber von vornherein an Restriktionen gebunden sein, die den Schutz des Bürgers garantieren. Löschungsvorschriften sind in diesem Zusammenhang genauso wichtig wie ein striktes Verbot, die zu Planungszwecken erhaltenen Angaben weiterzugeben. Ganz in diesem Sinn enthielt der im Sechsten Tätigkeitsbericht veröffentlichte Musterentwurf eines Datenschutzgesetzes eine Vorschrift über die Verarbeitung zu Planungszwecken. Sie ist seinerzeit nicht übernommen worden. Die Erfahrungen der letzten Jahre sprechen aber dafür, sich erneut eingehend mit der Möglichkeit einer Ergänzung des Datenschutzgesetzes auseinanderzusetzen (siehe auch: 2.1.8).

1.2.6 Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung personenbezogener Daten an die Kirchen hat, nicht zuletzt im Zusammenhang mit der geplanten Reform des Melderechts, Anlaß zu einer Reihe grundsätzlicher Überlegungen gegeben. Das Datenschutzgesetz (§ 12 Abs. 2) spricht die Übermittlung ausdrücklich an und bindet sie an die Bereitschaft der öffentlich-rechtlichen Religionsgesellschaften, „ausreichende“ Datenschutzmaßnahmen zu treffen. Insofern lag es nahe, sich damit zu beschäftigen, für welche Vorkehrungen sich die Kirchen bislang entschieden haben. Der Bericht gibt einen ausführlichen Überblick. Wohl gemerkt, das Datenschutzgesetz rechtfertigt es nicht, den Kirchen vorzuschreiben, wie sie sich zu verhalten

haben. Es ist ihre Aufgabe, den von ihnen für richtig gehaltenen Weg zu definieren und die von ihnen für angebracht angesehenen Maßnahmen näher zu umschreiben. Die öffentliche Verwaltung kann allerdings nicht umhin, sich mit diesen Vorkehrungen im einzelnen auseinanderzusetzen, um auch wirklich angeben zu können, ob ein „ausreichender“ Datenschutz vorliegt. Die staatliche Datenschutzgesetzgebung ist deshalb notwendiger Vergleichsmaßstab und insofern auch Konkretisierung der im Interesse des Betroffenen erforderlichen Mindestsicherung.

Das Datenschutzgesetz gibt aber gleichzeitig mit seiner Regelung zu erkennen, daß ein genereller Anspruch der Kirchen auf die bei der Verwaltung vorhandenen Angaben nicht besteht. Die rechtlich abgesicherten Informationserwartungen der Kirche sind in Art. 140 GG i. V. m. Art. 137 Abs. 6 WRV festgelegt. Jede darüber hinausgehende Anforderung muß sich nicht zuletzt strikt an die verfassungsrechtlich garantierte Glaubens- und Bekenntnisfreiheit halten. Zudem zeigen gerade die kirchlichen Datenschutzregelungen, wie wichtig es im Interesse der Betroffenen ist, Klarheit über die Verarbeitung im Rahmen kirchlicher Einrichtungen sowie der kirchlichen Presse zu gewinnen. Keines dieser Probleme ist neu. Jedes von ihnen gibt aber nach wie vor zu Meinungsverschiedenheiten Anlaß, die den Versuch, einen wirksamen Datenschutz sicherzustellen, belasten. Der Betroffene darf nicht unter den Folgen eines Kompetenzstreits leiden. Er muß vielmehr die Gewißheit haben, daß die Verarbeitung auch in diesem Bereich an den Respekt vor seiner persönlichen Integrität gebunden ist (siehe auch: Dritter Teil, 3.1 und 3.2).

1.3 Organisatorische Maßnahmen

1.3.1 Auskunftsanspruch und Übermittlungssperre

Der Datenschutz verlangt mehr als nur klar formulierte Verarbeitungsbedingungen. Seine Wirksamkeit hängt entscheidend von einer Reihe organisatorischer Maßnahmen ab, die es dem Bürger erleichtern sollen, seine gesetzlich garantierten Rechte wahrzunehmen. Ganz in diesem Sinn verpflichtet das Gesetz (§ 25) den Datenschutzbeauftragten, ein Register der Dateien zu führen, in denen personenbezogene Daten gespeichert werden. Dem Betroffenen wird damit eine Orientierungshilfe zur Verfügung gestellt. Er soll die Möglichkeit haben, zunächst eine zuverlässige Information über die speichernden Stellen zu

bekommen, um dann in Kenntnis der eigenen Lage sein Auskunftsrecht gezielt geltend zu machen. Doch was auf den ersten Blick ebenso selbstverständlich wie einfach erscheint, bereitet beträchtliche Schwierigkeiten. Die Vorarbeiten haben sich als überaus kompliziert erwiesen. Nicht nur, weil es kaum auf Anhieb gelingt, die für das Register erforderlichen Angaben von den speichernden Stellen zu erhalten, sondern auch und vor allem mit Rücksicht auf ihre Zahl. Nach dem gegenwärtigen Erfassungsstand haben in Hessen 2 981 speichernde Stellen 7 362 Dateien angemeldet. Es ist jedoch mit einem Endstand von rund 25 000 Dateien zu rechnen.

Diese Zahlen zwingen dazu, sich noch einmal intensiv mit dem Auskunftsrecht des Betroffenen auseinanderzusetzen. Schon der Hinweis auf die Hunderte möglicher Adressaten seines Informationsanspruchs wirkt lähmend. Kaum jemand dürfte bereit sein, den Aufwand an Mühe und Zeit auf sich zu nehmen, den eine wirklich detaillierte Auskunft verlangt. Zudem kann nicht immer vom Betroffenen eine Auswahl erwartet werden, die gleichsam zielsicher Schwerpunkte setzt. Dafür ist nicht zuletzt eine Kenntnis der öffentlichen Verwaltung erforderlich, die in den wenigsten Fällen vorhanden sein dürfte. Unter diesen Umständen gilt es, nach Auskunftsmodalitäten zu suchen, die der gesetzlichen Verpflichtung zur Offenlegung der Verarbeitung entgegenkommen.

Bezeichnend dafür sind die im Sicherheitsbereich angestellten Überlegungen. Der Betroffene darf nicht zum Opfer einer Kompetenzaufteilung werden, die er nicht zu durchschauen vermag, und die ihm letztlich die Chance nimmt, eine für ihn verständliche und vollständige Auskunft zu bekommen. Es kann mit anderen Worten nicht Aufgabe des Betroffenen sein, sich zunächst Klarheit über die unterschiedlichen Zuständigkeiten der einzelnen Sicherheitsbehörden zu verschaffen, um dann jede einzelne von ihnen anzugehen. Vielmehr ist die öffentliche Verwaltung verpflichtet, Auskunftsmechanismen zu entwickeln, die dem Betroffenen genau diese – das Auskunftsrecht letztlich gefährdende – Vorarbeit ersparen. Sie hat von Anfang an die bessere Übersicht, sie muß daher auch dafür sorgen, daß das Auskunftsrecht nicht an internen administrativen Komplikationen scheitert. Deshalb fragt es sich, warum es nicht möglich sein soll, etwa im Bereich der kriminalpolizeilichen Verarbeitung einen einzigen Adressaten anzugeben, der den Betroffenen

darüber informiert, ob und welche Angaben zu seiner Person von den Kriminalämtern des Bundes und der Länder verarbeitet werden. Wohlgermerkt, zur Diskussion steht nicht die auch und gerade vom Datenschutz verlangte sorgfältige Unterscheidung der Verfügungsbe-
 rechtigung über die einzelnen Datenbestände. Zur Debatte steht allein, wie die Auskunftsmo-
 dalitäten in Kenntnis der erforderlichen Abschottung der Situation des Betroffenen und seinen Erwartungen angepaßt werden können.

Ähnliche Betrachtungen lassen sich in allen Bereichen der öffentlichen Verwaltung anstellen. Bei strikter Aufrechterhaltung der unterschiedlichen Kompetenzen kommt es darauf an, im Zusammenhang mit der Auskunftserteilung Regelungen zu finden, die den Betroffenen nicht von vornherein abschrecken, sondern es ihm so leicht wie möglich machen, sich eine Übersicht zu verschaffen.

Nichts anderes gilt letztlich für die in § 16 a Hessisches Meldegesetz (HessMeldeG) vorge-
 sehene Übermittlungssperre. Auch hier steht eine für den Betroffenen überaus bedeutsame Datenschutzvorkehrung auf dem Spiel. Der Gesetzgeber überläßt es ihm, über die Ver-
 breitung der zu seiner Person verarbeiteten Angaben zu bestimmen. Er kann also, soweit er es für richtig hält, unter den in § 16 a HessMeldeG näher bestimmten Voraussetzungen den Zugriff Dritter ausschließen. Die Erfahrung zeigt freilich, daß die bloße Erwähnung der Übermittlungssperre im Gesetz nicht ausreicht. Kaum jemand nimmt von ihr Kenntnis, kaum jemand ist deshalb auch in der Lage, sie geltend zu machen. Dem Betroffenen daraus einen Vorwurf zu machen, wäre verfehlt. Seine Einstellung ist alles andere als verwunderlich. Er war es gewohnt, daß seine Daten weitergegeben werden, er sieht daher auch keinen Anlaß, von einem Recht Gebrauch zu machen, das der bisherigen Praxis zuwiderläuft. Wiederum muß es infolgedessen Aufgabe der Verwaltung sein, ihn auf die veränderte Rechtslage aufmerksam zu machen und ihm damit die Möglichkeit zu geben, Entscheidungen zu treffen, die das Gesetz von ihm erwartet.

Welche Bedeutung eine solche Information durch die Verwaltung hat, läßt sich am Umfang der bisherigen Auskunftssperren ablesen. In Gemeinden, die den Bürger unmittelbar angesprochen haben, gehen sie in die Hunderte. Dort hingegen, wo überhaupt nichts geschehen ist, sind es selbst bei Tau-
 senden von Einwohnern nicht einmal fünfzig.

Der Datenschutz setzt mithin auch ein ver-
 ändertes Verhalten dem Bürger gegenüber voraus. Die öffentliche Verwaltung muß das Gespräch mit ihm suchen, ihm verdeutlichen, welche Veränderungen sich vollzogen haben und ihm damit alle Information geben, die er braucht, um zu verstehen, welchen Unter-
 schied die Entscheidung des Gesetzgebers für den Datenschutz für ihn ausmacht (siehe auch: 2.2.2).

1.3.2 Datensicherung und Löschung

Zu den im Interesse eines wirksamen Daten-
 schutzes notwendigen organisatorischen Vor-
 kehrungen zählen auch Maßnahmen der
 Datensicherung. Die Erfahrung zeigt freilich,
 daß die Datensicherung unter Umständen in
 Widerspruch mit ihrer vom Gesetz angestreb-
 ten Schutzfunktion gerät. Das Beispiel der
 Log-Dateien ist bezeichnend genug. Sie
 ermöglichen es, fehlerhafte Verarbeitungsab-
 läufe zu wiederholen, aber auch festzustellen,
 wer bestimmte Angaben eingegeben, die
 Datenstation benutzt oder eine Übermittlung
 vorgenommen hat. Sie entsprechen insofern
 genau den Anforderungen, die das Gesetz in
 § 10 Abs. 1 aufstellt. Erst durch eine solche
 Protokollierung läßt sich der Verarbeitungs-
 prozeß exakt verfolgen und damit seine Kon-
 trolle sicherstellen. Die Existenz einer derar-
 tigen Datei wird allerdings dann problema-
 tisch, wenn dem Betroffenen ein Löschungs-
 anspruch zusteht. In letzter Konsequenz zielt
 er darauf ab, die speichernde Stelle zu ver-
 pflichten, die Daten zu vernichten, die sie
 nicht verarbeiten darf. Nur ist bislang dieser
 Erwartung nur im Zusammenhang mit der
 Originaldatei entsprochen worden. Die ge-
 setzlich unzulässige Speicherung besteht mit
 anderen Worten fort, wenngleich in einer
 besonderen Sicherungszwecken dienenden
 Datei. Dennoch ist die Gefahr für den Betrof-
 fenen nicht zu übersehen. Was zunächst in
 seinem Interesse geschieht, kann sehr leicht zu
 seinem Nachteil genutzt werden. Die ur-
 sprüngliche funktionale Trennung der Dateien
 reicht deshalb nicht aus. Vielmehr bedarf es
 besonderer Vorschriften, die eine Zweckent-
 fremdung der Sicherungsdatei von vornherein
 ausschließen. Die Grundlage dafür gibt § 10
 Abs. 2 HDSG ab. Über die dort enthaltene
 Verordnungsermächtigung gilt es einer Um-
 kehrung der gesetzlichen Sicherungsintention
 zuvorzukommen (siehe auch: 2.4.2).

1.3.3 Dezentralisierung der Verarbeitung

Lange Zeit schien die technische Entwicklung
 eine Zentralisierung der Verarbeitung nahe-

zulegen. Der Hessische DV-Verbund ist ein sichtbares Zeichen dafür. Für den Datenschutz ein nicht unwichtiger Vorgang. Die Zentralisierung erleichtert die Kontrolle. Die Überwachung konzentrierte sich weitgehend auf die sechs Rechenzentren des Verbundes mit der Konsequenz, daß relativ schnell und zuverlässig ein Überblick über die jeweils getroffenen Sicherungsmaßnahmen gewonnen und ihre Wirksamkeit geprüft werden konnte.

Eben diese Entwicklung scheint sich mittlerweile umzukehren. Technisch bereitet es inzwischen keine Schwierigkeit, kleinere und leistungsfähigere Komponenten der Datenverarbeitung zu konstruieren. Die Konsequenz ist eine fortschreitende Rückverlegung der Verarbeitung in die einzelnen Verwaltungsbereiche. In dem Maße aber, in dem dies geschieht, verändern sich auch die Anforderungen an die Kontrolle durch den Datenschutzbeauftragten. Die Dezentralisierung vermindert die Transparenz der Sicherungsmaßnahmen. Zudem fallen sie in zunehmendem Maße unterschiedlich aus und werden nach Gesichtspunkten getroffen, die weit weniger vom Datenschutz als von den für die speichernde Stelle entstehenden Kosten geleitet werden.

Die Dezentralisierung ist deshalb, jedenfalls in ihrer gegenwärtigen Form, nicht wider-

spruchslos hinzunehmen. Mittel für dezentral einzusetzende Anlagen dürfen solange nicht bewilligt werden, wie nicht Klarheit darüber besteht, ob die jeweils erforderlichen Sicherungsmaßnahmen getroffen werden können. Die möglichen technischen Vorteile reichen für sich genommen nicht aus, um die Dezentralisierung zu rechtfertigen. Sie wird erst in dem Augenblick zulässig, in dem auch feststeht, daß die Verlagerung der Verarbeitung nicht auf Kosten des Betroffenen geschieht. Der Datenschutz versperrt insofern den Zugang zu anderen Verarbeitungsmodalitäten, die zwar aus der Perspektive der speichernden Stellen von Nutzen sind, aber nicht dem vom Gesetz im Interesse des Bürgers gestellten Anforderungen an den Verarbeitungsprozeß Rechnung tragen (siehe auch: 2.4.5).

Jeder der hier erwähnten Punkte bestätigt: Regierung und Parlament haben mit ihren Entscheidungen den Rahmen für einen wirkamen Schutz des Bürgers abgesteckt. Die Anforderungen sind dennoch nach wie vor beträchtlich. Es gilt, sich ihrer bewußt zu sein und den vorhandenen Datenschutz durch Regelungen zu ergänzen, die den Respekt vor dem Bürger noch deutlicher und noch überzeugender zum Ausdruck bringen.

2. ZWEITER TEIL

2. Zweiter Teil

Datenschutzprobleme – Erfahrungen und Beispiele

2.1. Administrative und wissenschaftliche Befragungen

2.1.1 „Gasöldatai“/Abgabenordnung

Ein nicht einfach zu lösender Konflikt zwischen Vorschriften der Abgabenordnung und dem Datenschutz ergab sich aus einem Amtshilfeersuchen des Hessischen Ministers der Finanzen an den Hessischen Minister für Landesentwicklung, Umwelt, Landwirtschaft und Forsten wegen der Übermittlung von Daten aus der sogenannten „Gasöldatai“. Diese Datei dient (vgl. I 4.1.1.3 e, S. 25) der Durchführung des Gasölverwendungsgesetzes. Mit ihrer Hilfe wird die von der jeweiligen Betriebsgröße abhängige Berechtigung eines Landwirts zum verbilligten Bezug von Gasöl festgestellt. Der Finanzminister hatte darum gebeten, ihm im Wege der Amtshilfe gemäß § 111 ff. der Abgabenordnung (AO) die Daten der ca. 28 500 Inhaber landwirtschaftlicher Betriebe über 10 ha Betriebsgröße in Hessen zu übermitteln. Mit Hilfe dieser Daten sollte festgestellt werden, ob die Steuerpflichtigen ihrer Steuerpflicht genügt haben; soweit dies nicht der Fall war, sollten die noch ausstehenden Steuern für die zurückliegenden fünf Jahre nacherhoben werden. Da die Daten von den Landwirten zu dem Zweck an das Landwirtschaftsamt übermittelt worden waren, verbilligtes Gasöl für ihre Betriebe beziehen zu können, hatte der Landwirtschaftsminister Bedenken, die Daten entsprechend dem Amtshilfeersuchen für einen anderen Zweck zu übermitteln.

Es muß von vornherein betont werden, daß die Berechtigung des Finanzministers zu dem Amtshilfeersuchen aufgrund der Abgabenordnung außer Zweifel steht, und daß es auch nicht darum gehen konnte, säumige Steuerzahler dem Zugriff der Finanzbehörden zu entziehen. In diesem Zusammenhang muß jedoch, so scheint mir, zweierlei überlegt werden. Einerseits überläßt der Bürger seine

Daten im Hinblick auf einen ganz bestimmten Zweck und erwartet auch, daß sie grundsätzlich nur im Zusammenhang mit diesem Zweck verarbeitet werden. Bundes- und Landesgesetzgeber haben gerade mit Rücksicht auf diese Zweckbindung die Verarbeitung von einer gesetzlichen Grundlage oder vom Einverständnis der Betroffenen abhängig gemacht. Im einen wie im anderen Fall soll der Bürger die Chance haben zu erkennen, warum seine Daten verarbeitet werden sollen und mit welchem Ziel. Nur unter dieser Voraussetzung kann der Bürger nicht nur entscheiden, ob er seine Daten zur Verfügung stellen soll – eine Feststellung, die gerade bei einer freiwilligen Erhebung von Bedeutung ist – sondern auch seine gesetzlich abgesicherten Kontrollrechte wirksam ausüben. So gesehen, erscheint die vom Finanzminister gewünschte Datenübermittlung problematisch. Der Bürger überläßt seine Daten freiwillig, mit Rücksicht auf eine bestimmte Leistung – die Gasölverbilligung – und geht wohl in aller Regel davon aus, daß die Überlassung seiner Daten keinen anderen Zweck hat als die Durchführung der beantragten Leistung. Andererseits dürfen gerade in diesem Zusammenhang die Vorschriften der Abgabenordnung nicht übersehen werden. Die darin vorgesehene Auskunftspflicht der Behörden (§ 93 Abs. 1 AO) und die Einschränkung der Schweigepflicht (§ 105 Abs. 1 AO) ergeben, daß der Gesetzgeber dem Auskunftsrecht der Finanzbehörden eine ganz besondere Bedeutung beimißt. Auch unter Berücksichtigung des für den Datenschutz maßgeblichen Grundsatzes der Zweckbindung kann deshalb die geforderte Amtshilfe nicht verweigert werden. Die Daten waren infolgedessen entsprechend dem Ersuchen des Hessischen Ministers der Finanzen zur Verfügung zu stellen.

Mit Rücksicht auf das Interesse der Bürger an einer für sie durchschaubaren Verarbeitung ihrer Daten habe ich allerdings für die Zukunft angeregt, das Erhebungsformular um einen Vermerk zu ergänzen, der die mögliche Übermittlung der Daten an die Finanzbehörden für steuerliche Zwecke offenlegt. Der Landwirtschaftsminister hat diese Anregung aufgegriffen und hat die Erhebungsformulare entsprechend ergänzt.

2.1.2 Datenverarbeitung bei Beratungsstellen nach § 218 StGB

Verschiedentlich ist durch Abgeordnete und besorgte Bürger die Frage aufgeworfen worden, ob personenbezogene Daten von Frauen, die sich in städtischen Sozialberatungsstellen oder bei anderen Beratungsinstitutionen, wie Pro Familia und Caritas, einer Schwangerschaftsberatung nach § 218 BStGB unterzogen haben, in Hessen – wie anderenorts geschehen – dann auch in Sozialämtern, beim Regierungspräsidenten oder gar beim Sozialminister gespeichert bzw. an diese übermittelt werden.

Ich habe diesen Sachverhalt zum Anlaß genommen, den Sozialminister um eine Überprüfung der Datenverarbeitung im Zusammenhang mit der Schwangerschaftsberatung zu bitten. Der Sozialminister hat seine Nachforschungen noch nicht abgeschlossen. Meine Überprüfung der Beratungsstellen in einer hessischen Großstadt, die notwendig nur exemplarischen Charakter haben konnte, hat jedoch Befürchtungen, zu der die Praxis in einigen anderen Bundesländern Anlaß gegeben hat, nicht bestätigen können. Die von mir überprüften Beratungsstellen halten die Personalien und die Gründe für die Feststellung einer Indikation in einer Beratungsakte fest, die keine Datei ist und darüber hinaus der ärztlichen Schweigepflicht unterliegt. Im übrigen findet die Beratung, sofern betroffene Frauen dies wünschen, anonym statt. Sie wird der Schwangeren oder mit ihrer Zustimmung einem von ihr benannten Arzt auf Verlangen schriftlich bestätigt. Gemäß § 3 Abs. 4 des Gesetzes zur Ausführung der §§ 218 b und 219 des Strafgesetzbuchs und des Art. 3 des 5. Gesetzes zur Reform des Strafrechts vom 2. Mai 1979 GVBl. S. 273 hat der Träger einer anerkannten Beratungsstelle die Mitglieder und Beauftragten der Beratungsstelle sowie deren berufsmäßig tätige Gehilfen und Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind, über ihre Pflicht zur Verschwiegenheit sowie über ihr Zeugnisverweigerungsrecht zu unterrichten und sie auf die strafrechtlichen Folgen einer Verletzung der Geheimhaltungspflicht hinzuweisen. Die Ratsuchenden sollen nach diesem Gesetz ebenfalls über die Schweigepflicht der Beratenden unterrichtet werden. Die Beratungsstellen werden vom Regierungspräsidenten, die beratenden Ärzte von der Landesärztekammer Hessen darauf hin überwacht, ob sie die für die Beratung geltenden gesetzlichen Bestimmungen einhalten. Personenbezogene

Angaben der ratsuchenden Frauen dürfen an dritte Stellen nicht übermittelt werden, und die Beratungsstellen haben lediglich dem Regierungspräsidenten jährlich in Form einer schriftlichen Berichts Auskunft über die Zahl der Beratungen sowie über Alter, Familienstand, Wohnsitz und Nationalität der Beraternen, jedoch ohne Namensnennung eine statistische Mitteilung zu machen (vgl. § 4 Abs. 2 des hessischen Gesetzes zur Ausführung der §§ 218 b und 219 StGB). Im Ergebnis konnte ich daher für die Beratungsstellen dieser hessischen Großstadt feststellen, daß in Hessen keine personenbezogenen Daten von den Beratungsstellen an Dritte übermittelt werden, und daß die betroffenen Datensicherungsmaßnahmen zur Aufbewahrung der Akten ausreichen. Eine abschließende Beurteilung dieser Sachlage für ganz Hessen ist allerdings erst nach dem in Aussicht gestellten Bericht des Sozialministers möglich.

2.1.3 Sozialbericht bei Suchtkranken

Im Rahmen ihrer Aufgaben erstatten die Rentenversicherungsträger den Krankenkassen die Kosten für die Rehabilitation von Suchtkranken – Alkoholiker, Medikamentensüchtige, Drogensüchtige – in Spezialkrankenhäusern. Mit dem Inkrafttreten des Kostendämpfungsgesetzes ergab sich die Notwendigkeit, vor Entscheidung über die Entwöhnungsbehandlung die vermutlichen Erfolgsaussichten einer Rehabilitation zu prüfen. Aufgrund einer Vereinbarung zwischen den Krankenversicherungsträgern und den Rentenversicherungsträgern „über die Zusammenarbeit bei der Rehabilitation Abhängigkeitskranker“ wird seit April 1979 neben den üblichen ärztlichen Gutachten auch ein ausführlicher „Sozialbericht“ von den Suchtberatungsstellen verlangt. Die Suchtberatungsstellen werden in der Regel in privat-rechtlicher Form von den Trägern der freien Wohlfahrtspflege (paritätischer Wohlfahrtsverband, Diakonisches Werk, Caritas usw.) betrieben. Diese Stellen sehen durch die Verpflichtung, einen solchen „Sozialbericht“ zu erstellen, den Erfolg ihrer Arbeit gefährdet, da hier sehr empfindliche medizinische und soziale Daten des Suchtkranken, die dem Arzt- und dem Sozialgeheimnis unterliegen, lediglich zur Kontrolle der Wirtschaftlichkeit von Maßnahmen weitergegeben werden.

Das ursprünglich zweiseitige Formular ist inzwischen als „Sozialbericht – psychosoziale Grunddaten –“ auf vier DIN A 4-Seiten mit über 60 Fragen und ausführlichen Stellung-

nahmen zur Betreuung durch die Beratungsstellen, zur Sozialanamnese des Betreuten und zu seiner Persönlichkeit sowie zur sozialen Situation der Bezugspersonen angewachsen. Es enthält neben Fragen zur Person solche beispielsweise über Konfession, Staatsangehörigkeit, Unterhaltsverpflichtungen, Arbeitgeber, Entmündigungen, Zahl der Kinder, Wohn- und finanzielle Verhältnisse, frühere Krankheiten, Suicid-Versuche, Verhalten unter Einfluß von Suchtmitteln, seelisch-geistige Veränderungen, Straffälligkeit und Motivation. Auch über die charakterliche Bewertung der Bezugspersonen soll der Fragebogen Auskunft geben. Formal wird der Forderung nach Wahrung des Arzt- bzw. des Sozialgeheimnisses und des Datenschutzes durch Rechnung getragen, daß die Einverständniserklärung des Betreuten zur Weiterleitung der Daten des „Sozialberichts“ an den Leistungsträger und das Fachkrankenhaus dem Fragebogen beigelegt wird. Diese formale Betrachtungsweise und das bei diesem „Sozialbericht“ angewandte Verfahren insgesamt können den Forderungen des Datenschutzes nicht genügen. Die Einwilligung des Betroffenen, die darauf gerichtet ist, durch Teilnahme an einer Entziehungskur von seiner Sucht befreit zu werden, kann nicht sein Einverständnis dazu bedeuten, daß die über ihn erhobenen sensitiven medizinischen Daten, die „Sozialanamnese“, sowie die Beurteilungen der Suchtberatungsstelle über ihn selbst und seine Bezugspersonen zu anderen Zwecken als dem der Rehabilitation übermittelt werden dürfen. Hier würde der den gesamten Datenschutz bestimmende Grundsatz der Zweckbindung verletzt: Die Prüfung der Wirtschaftlichkeit und Zweckmäßigkeit einer beantragten Entziehungskur ist ein anderer Zweck als die Durchführung der Rehabilitation durch das Spezialkrankenhaus. Einmal ist es zweifelhaft, ob außer den behandelnden Ärzten des Spezialkrankenhauses andere Stellen fachlich in der Lage sind, die Erfolgsaussichten einer solchen Entwöhnungskur zu beurteilen. Aber selbst wenn die Rentenversicherungsträger über entsprechend qualifiziertes Fachpersonal verfügen, erscheint mir eine so umfangreiche Datenübermittlung an sie, wie dies der „Sozialbericht“ ermöglicht, für den Zweck der Wirtschaftlichkeitsprüfung nicht gerechtfertigt. Zu Recht wird von den Kritikern dieses Verfahrens darauf hingewiesen, daß auch Rheuma- oder Asthmakranke, die eine Kur beantragen, nicht derart umfangreich nach ihren persönlichen Verhältnissen befragt werden.

Aus diesen Überlegungen sind einige Suchtberatungsstellen dazu übergegangen, die Verwendung des „Sozialberichts“ abzulehnen, und zwar „wegen rechtlicher Bedenken und aus grundsätzlichen Erwägungen des Datenschutzes“. Sie leiten einen ausführlichen Bericht mit der Sozialanamnese dem Fachkrankenhaus unmittelbar zu. Auch bei diesem Verfahren besteht die Möglichkeit, daß der Versicherungsträger bei Zweifeln an den Erfolgsaussichten einer Rehabilitationsbehandlung sich vor deren Beginn bei den zuständigen Ärzten des Fachkrankenhauses über den möglichen Erfolg der Behandlung vergewissern kann. Wie bei einer ersten Fühlungnahme mit den Datenschutzbeauftragten der anderen Bundesländer und dem Bundesbeauftragten für den Datenschutz zu erfahren war, verfährt das Land Bayern bereits in der oben geschilderten Weise. Weitere Bundesländer beabsichtigen, diesem Beispiel zu folgen.

Für die Entscheidung des Rentenversicherungsträgers darüber, ob er die Kosten für eine Rehabilitationsbehandlung übernimmt, muß er lediglich wissen, ob die Behandlung hinreichende Aussicht auf Erfolg bietet. Er muß also lediglich das Ergebnis der medizinischen Untersuchung sowie der Sozialanamnese kennen, nicht aber die diesen zugrundeliegenden Daten, also den Befund selbst. Die aus der Sicht des Datenschutzes akzeptierte Lösung kann also nur in einem Verfahren liegen, wie es bereits im Arbeitsrecht praktiziert wird: Bei der betriebsärztlichen Untersuchung von Arbeitnehmern wird unterschieden zwischen dem Befund- und dem Bescheidbogen. Der Befundbogen mit der Anamnese, der Diagnose und den Angaben zur Therapie steht nur dem Arzt zur Verfügung; der Arbeitgeber erhält dagegen nur den Bescheidbogen, in dem mitgeteilt wird, ob und ggf. unter welchen Voraussetzungen der Arbeitnehmer für eine bestimmte Tätigkeit geeignet ist. Diese auf den Bestimmungen der §§ 3 Abs. 2 und 8 Abs. 1 S. 2 des Betriebsärztegesetzes vom 12. Dezember 1973 (BGBl. I S. 1885) beruhende Praxis muß auch Richtschnur für das hier kritisierte Verfahren sein. Ich rege daher an, die bestehenden gesetzlichen Bestimmungen und vertraglichen Vereinbarungen in der Weise zu ändern, daß künftig die Rentenversicherungsträger nur noch über die Fachklinik bzw. einen Facharzt des Gesundheitsamtes das Ergebnis der Untersuchung eines Suchtkranken im Hinblick auf dessen Rehabilitationsfähigkeit mitgeteilt bekommen. Darüber hinaus sollten alle

Verfahren, bei denen lediglich aufgrund des Kostendämpfungsgesetzes zur Überprüfung der Wirtschaftlichkeit einer Maßnahme medizinische Daten übermittelt werden, einer entsprechenden Prüfung und Abänderung unterzogen werden. Ich verweise in diesem Zusammenhang auf meine Ausführungen zur Datenerhebung und Datenübermittlung bei Sozialstationen (siehe 2.1.4).

2.1.4 Datenübermittlung bei Sozialstationen

Eine bei einer städtischen Sozialstation in der häuslichen („mobilen“) Krankenpflege tätige Krankenschwester beschwerte sich bei mir über ihre Verpflichtung zur Übermittlung von Patientendaten zum Zwecke der Abrechnung. Der Beschwerde liegt folgende Situation zugrunde: Nach § 185 der Reichsversicherungsordnung (RVO) besteht die Möglichkeit, die Behandlung („Hilfe und Wartung“) und Betreuung von Kranken außerhalb des Krankenhauses im Wege der mobilen Krankenpflege durch eine, meist städtische, Sozialstation vornehmen zu lassen. Im Hinblick auf die enormen Kosten der stationären Krankenpflege wird von dieser Möglichkeit reger Gebrauch gemacht; die Gemeinden werden durch Fördermittel des Landes und zum Teil auch der Kreise zur Errichtung solcher Sozialstationen ermuntert. Das der Beschwerde zugrundeliegende Problem liegt in der Form der Abrechnung der Krankenpflegeleistungen: Um den Ersatz der durch ihre Sozialstationen erbrachten Leistungen von den Versicherungsträgern zu erhalten, sind die Gemeinden verpflichtet, Nachweise über die erbrachten Leistungen zu führen. Diese Leistungsnachweise enthalten außer dem Namen und der Anschrift des Patienten und den Daten der jeweiligen Besuche der Schwester Angaben über „volle Grundpflege“ oder „Teilgrundpflege“, Anlegung von Verbänden, Spülungen, Einlegen eines Katheters, Injektionen, Verabreichung von Medikamenten, „Darmeinlauf“ usw. Diese Angaben werden von der Schwester an das städtische Sozialamt, von diesem weiter an den Versicherungsträger übermittelt. Die Beschwerdeführerin sah in dieser Übermittlung medizinischer Daten die Gefahr einer Verletzung ihrer Schweigepflicht gemäß § 203 Strafgesetzbuch (StGB) und darüber hinaus der Bestimmungen von § 12 HDSG.

Eine zwischen den Wohlfahrtsverbänden, den Kirchen und den kommunalen Spitzenverbänden einerseits und den Verbänden der Versicherungsträger abgeschlossene „Rahmenver-

einbarung zur Erbringung der häuslichen Krankenpflege im Rahmen des § 185 RVO“ sowie eine „Vereinbarung über Vergütungs- und Rechnungslegung der häuslichen Krankenpflege gemäß § 4 der Rahmenvereinbarung“ sehen vor, daß die Vergütung sowohl nach Einzelleistung wie auch im Wege einer Pauschale vereinbart werden kann. In dem der Beschwerde zugrunde liegenden Falle ist es zu der von der Stadt angestrebten Pauschalabrechnung wegen der Weigerung des zuständigen Versicherungsträgers nicht gekommen. Bei der Vergütungs- und Rechnungslegung im Wege der Einzelabrechnung läßt sich aber eine Erfassung und Übermittlung einzelner Patientendaten zum Zwecke der Abrechnung – ähnlich wie dies bereits von den Krankenhäusern praktiziert wird – nicht vermeiden. Die beteiligten Gemeinden und Krankenkassen sind auch nach den Vorschriften der RVO befugt, eine solche Abrechnungsweise zu vereinbaren. Formal betrachtet, war daher die Verpflichtung der Krankenschwester zur Führung eines Leistungserfassungsnachweises und zur Übermittlung der erfaßten Daten an das städtische Sozialamt nicht zu beanstanden. Trotzdem ist dieses Verfahren aus der Sicht des Datenschutzes nicht ohne Bedenken: Hier werden Daten, die der Patient zur Erlangung einer Pflege- oder Betreuungsleistung – mehr oder weniger unfreiwillig – der Sozialstation gegeben hat, aus dem Bereich des ärztlichen Hilfspersonals an die städtische Sozialverwaltung und von dieser weiter an eine Krankenversicherung gegeben. Hier muß die Frage gestellt werden, ob nicht eine Änderung der gesetzlichen Bestimmungen, die eine so weitgehende Übermittlung sehr empfindlicher Patientendaten zulassen, zugunsten einer Pauschalabrechnung notwendig ist. Dabei muß nicht zuletzt auch die Frage nach der Wirtschaftlichkeit eines so erheblichen Aufwandes, wie er bei Kommunen und Krankenkassen für die Einzelabrechnung erforderlich ist, gestellt werden.

2.1.5 Medizinisch-psychologische Untersuchungen

Konflikte besonderer Art entstehen dann, wenn wissenschaftliche Tests zur Beurteilung der Persönlichkeitsstruktur, bestimmter Neurotizismen und abweichenden Sexualverhaltens zur Grundlage von Vollzugsentscheidungen gemacht werden. Dies ist vor allen Dingen bei den medizinisch-psychologischen Untersuchungen, sog. „Idiotentests“, für solche Führerscheinbewerber deutlich geworden, denen die Fahrerlaubnis entzogen worden war, und

die sich einer medizinisch-psychologischen Untersuchung unterziehen mußten. Grundsätzlich wird nicht bestritten, daß psychologische Untersuchungen zur Überprüfung der Fahrtauglichkeit nötig sind. Vielmehr geht es um die Methoden, mit denen die Führerscheinbewerber befragt werden.

Rechtsgrundlage für diese medizinisch-psychologische Untersuchung ist der § 15 StVZO, in dem es heißt, daß zur Wiedererteilung der Fahrerlaubnis in der Regel Gutachten beigebracht werden müssen. In Hessen wurden diese Gutachten in der Regel durch die medizinisch-psychologische Untersuchungs- und Beratungsstelle der Staatlichen Technischen Überwachung Hessen aufgrund standardisierter Tests erstattet. Dabei wurden in Einzelfällen neben verkehrspsychologischen Tests auch Fragebogen benutzt, die für die Begutachtung psychisch kranker Personen im klinischen Bereich entwickelt worden sind. Diese Tests wie MMPI (Minnesota Multiphasic Personality Inventory) und MMQ (Maudley's Medical Questionnaire) geben zwar nach Auffassung von Psychologen eine gewisse Gewähr für das Erkennen psychopathologischer oder neurotischer Symptome, können aber keine gültige Grundlage zur Beurteilung der Fahrtauglichkeit abgeben. Anders ausgedrückt: Es gibt keine Bewährungsuntersuchung dieser Tests, die eine spezifische Validität für Verkehrs- und Fahrtauglichkeit nachweisen können. Hier setzt denn auch die datenschutzrechtliche Problematik ein: Wenn feststeht, daß andere und wesentlich mehr Daten erhoben werden, als zur Beurteilung der Fahrtauglichkeit erforderlich ist, bzw. die Tests insofern nicht geeignet sind, spezifische Aussagen über Fahrtauglichkeit von Betroffenen zu machen, dann stellt sich die Frage, ob diese Datenverarbeitung in standardisierten Testbatterien noch mit dem Datenschutzgesetz zu vereinbaren bzw. von § 15 StVZO als rechtlicher Basis gedeckt ist. Denn eine umfassende Analyse der Persönlichkeit des betroffenen Bürgers zu erstellen, ist nicht die Aufgabe einer staatlichen Behörde, die lediglich gutachterlich dazu Stellung nehmen soll, ob die für die Führerscheinausstellung zuständige Behörde dem Betroffenen eine Fahrerlaubnis erteilen kann.

Eine kleine Anfrage im Landtag und meine Intervention haben dazu geführt, daß der Hessische Minister für Wirtschaft und Technik die Verwendung dieser Fragebögen bei der medizinisch-psychologischen Untersuchung der Technischen Überwachung Hessen untersagt hat.

Die Konsequenz für alle staatlichen Stellen, die standardisierte Persönlichkeitstests verwenden und Vollzugsfolgen an deren Auswertung knüpfen, ist, daß nur solche Tests verwandt werden dürfen, die eine spezifische Validität für den Zweck besitzen, der erreicht werden soll.

Mit anderen Worten: Derjenige, der eine Fahrerlaubnis begehrt, darf nur danach gefragt werden, was zur Erteilung der Führerscheinerteilung erforderlich und geeignet ist. Jedes Überschreiten jener Informationsmenge ist unverhältnismäßig und beeinträchtigt den Bürger in seinem allgemeinen Persönlichkeitsrecht. Anders ist die Frage nur zu beurteilen, wenn der Betroffene selbst sich freiwillig einer solchen Befragung, z. B. im Zusammenhang mit einer ärztlichen Behandlung unterzieht. Dies gilt jedoch in der Regel nicht für die Voraussetzungen zur Erteilung einer Fahrerlaubnis. Die meisten Bürger sind in der heutigen Industriegesellschaft beruflich darauf angewiesen, eine Fahrerlaubnis zu besitzen. Von einer freiwilligen Unterwerfung unter eine solche Befragung kann daher normalerweise nicht die Rede sein.

2.1.6 Übermittlung von Einwohnerdaten an Adreßbuchverlage

Das Problem der Übermittlung von Einwohnerdaten an Adreßbuchverlage ist auch im abgelaufenen Berichtsjahr wiederholt an mich herangetragen worden. Zur Klarstellung der Situation sei noch einmal darauf hingewiesen, daß mit § 16 a des Hessischen Meldegesetzes die Übermittlung personenbezogener Daten aus dem Melderegister der Städte und Gemeinden an Stellen außerhalb des öffentlichen Bereichs abschließend geregelt ist¹⁾. Trotzdem scheinen die Probleme nicht völlig ausgeräumt. Dazu zwei Beispiele:

Eine kreisfreie Stadt hat aufgrund vertraglicher Vereinbarung mit einem Adreßbuchverlag seit 1964 regelmäßig Einwohnerdaten zur Herausgabe eines Adreßbuchs übermittelt. Nach Inkrafttreten des Hessischen Datenschutzgesetzes teilte sie dem Verlag mit, daß sie sich aus datenschutzrechtlichen Erwägungen und aus Gründen des Steuergeheimnisses nach § 30 der Abgabenordnung nicht in der Lage sehe, weiterhin die Anschriften der Grundstückseigentümer zu übermitteln. Der Verlag hat daraufhin von sich aus alle ihm aus alten Adreßbüchern bekannten Grundstücks-

¹⁾ Siehe auch Erlasse des Hessischen Ministers des Innern, Az.: III A 3 - 23 a 02 vom 21. Juli 1978 und 2. Oktober 1978.

eigner mit einem amtlich wirkenden Formbrief angeschrieben und um Mithilfe bei der „Ergänzung und Überprüfung der uns vorliegenden amtlichen Unterlagen“ gebeten. Zu diesem Zweck sollten dem Anschreiben beigefügte Hauslisten, welche Name und Anschrift des Hauseigentümers bzw. Verwalters und aller Bewohner sowie Berufsbezeichnung und Telefonanschluß enthielten, „zur eigenhändigen Eintragung zirkulieren“.

Auf meine Anregung hin hat der Magistrat der kreisfreien Stadt den Verlag auf die Unzulässigkeit seines Handelns hingewiesen, die sofortige Einstellung der Aktion gefordert und die Herausgabe der bereits erhobenen Daten verlangt. Die Bevölkerung wurde in einer umfangreichen Pressenotiz in den örtlichen Tageszeitungen auf die Rechtsauffassung der Stadt hingewiesen. Zur Prüfung, inwieweit der Verlag gegen die Bestimmung des Dritten Abschnitts des Bundesdatenschutzgesetzes verstoßen hat, habe ich die zuständige Aufsichtsbehörde bei dem Regierungspräsidenten in Darmstadt eingeschaltet.

Anders ein Fall in Nordhessen: Dort hat eine Stadtverwaltung durch Veröffentlichung in den Tageszeitungen darauf hingewiesen, daß sie beabsichtige, zusammen mit einem Verlag ein Adreßbuch herauszugeben. Gleichzeitig wies sie die Bürger auf das Sperrrecht nach § 16 a des Hessischen Meldegesetzes hin. Der Verlag seinerseits zeigte durch ein Inserat in den gleichen Tageszeitungen an, daß Korrekturlisten zur Einsicht auslügen. In das Adreßbuch aufgenommen werden sollten nur solche Einwohner, die weder von ihrem Sperrrecht Gebrauch gemacht hatten noch eine Korrektur in den ausgelegten Listen verlangten.

Die umfassende und rechtzeitige Information der Einwohner durch die beteiligten Stellen hat hier zu einer befriedigenden Lösung des Problems geführt.

2.1.7 Wissenschaftliche Forschung und Datenschutz

Der Konflikt zwischen Wissenschaftssystem und Datenschutz hat sich im Berichtszeitraum eher verschärft anstatt gemildert. Eine Auflösung der Fronten konnte man zunächst deshalb erwarten, weil das neue Hessische Datenschutzgesetz in § 15 als erstes eine bereichsspezifische Regelung für die Datenverarbeitung im Zusammenhang mit wissenschaftlicher Forschung enthielt. Nach den praktischen Erfahrungen mit dieser Regelung kann man feststellen, daß die Behörden ohne beratende Hilfe des Datenschutzbeauftragten

ebensowenig in der Lage waren, diese Bestimmung zutreffend anzuwenden, wie in der Forschung der Gedanke des Datenschutzes erst allmählich eine entsprechende Akzeptanz gewann. Dafür sind verschiedene Gründe ausschlaggebend. Die meisten Ersuchen an Behörden, Daten an Institutionen mit der Aufgabe unabhängiger wissenschaftlicher Forschung zu übermitteln, richten sich auf Adressen von Einwohnern aus dem Einwohnermelderegister mit dem Zweck, Stichproben für Repräsentativbefragungen zu ziehen. Die rechtliche Beurteilung, ob Daten aus dem Einwohnermelderegister an Forschungsinstitute weitergegeben werden können, richtet sich aber nach § 16 a des Hessischen Meldegesetzes. Da die empirische Forschung Auskünfte über eine Vielzahl von Einwohnern begehrt, unterliegt eine solche Gruppenauskunft der Regelung des § 16 a Abs. 3 des Hessischen Meldegesetzes. Diese Bestimmung sieht vor, daß eine Gruppenauskunft nur erteilt werden darf, wenn ein öffentliches Interesse vorliegt. Die Feststellung des öffentlichen Interesses obliegt dem Bürgermeister bzw. Oberbürgermeister als örtlich zuständige Meldebehörde. Aus meiner Beobachtung folgt, daß die unterschiedliche Konkretisierung des öffentlichen Interesses im Rahmen der staatlichen Weisungsaufgabe im Meldewesen zu großen Unsicherheiten bei der Anwendung des § 16 a sowohl bei den Meldebehörden wie bei den Forschungsinstituten geführt hat. Mit anderen Worten: Der Datenzugang für die wissenschaftliche Forschung ist potentiell gefährdet. Die Unsicherheit einer Entscheidungslage führt nach meiner Erfahrung bei nachgeordneten Behörden zu einer Entscheidung, von der die entscheidende Stelle wahrscheinlich keine politischen oder rechtlichen Nachteile zu erwarten hat. Im Ergebnis folgte häufig daraus eine Entscheidung zu Lasten wissenschaftlicher Forschung. Diese Tendenz wird noch verstärkt durch das Argument, daß die Meldebehörden aus Gesichtspunkten der Verwaltungsökonomie nicht in der Lage sind, den an sie gerichteten Anforderungen um Datenübermittlung nachzukommen. Die Voraussetzungen für die erforderliche Rechtssicherheit sind damit in Frage gestellt. Obwohl das Datenschutzgesetz die unmittelbare Verantwortlichkeit der Behörden für den Datenschutz in ihrem Geschäftsbereich festschreibt, vergeht keine Woche, ohne daß beim Datenschutzbeauftragten um „Entscheidungshilfe“ in Fragen des § 16 a und seiner Konkurrenz zu § 15 HDStG nachgesucht wird.

Wissenschaftspolitisch kann ein solches Abschneiden der Informationsströme an die empirische Forschung zu erheblichen Nachteilen für die empirische Forschung in Deutschland führen; einzelne Wissenschaftslobbyisten sagen gar scherzhaft das Erliegen ganzer Wissenschaftszweige in der Bundesrepublik voraus. Solche Schwarzmalerei führt allerdings kaum zu einer angemessenen Problemlösung. Verfassungsrechtlich ist ein versiegender Informationsstrom von der staatlichen Administration zu unabhängigen Forschungsinstitutionen nicht weniger gravierend als die kurzorische wissenschaftspolitische Beurteilung. Wissenschaftsfreiheit umfaßt nämlich ganz sicher nicht nur die institutionelle Garantie der Wissenschaft und komplementär dazu einen Schutz des Forschers vor staatlichen Eingriffen in die Forschung. Auch die Freiheit der Betätigung gehört zum Kernbestand der Wissenschaftsfreiheit im Sinne des Grundgesetzes. Dieser Kernbereich kann berührt werden, wenn der Datenzugang verwehrt wird. Noch ist dieses Stadium nicht erreicht. Ich würde jedoch die verfassungsrechtlich verbürgte Informationsstruktur in Gefahr sehen, wenn die staatliche Administration ihre Informationen und Daten in staatlichen Datenbanken monopolisiert. Eine derartige Entwicklung könnte auf lange Sicht zu einer Störung eines höchst empfindlichen gesamtgesellschaftlichen Informationsgleichgewichts führen: Wenn das Wissenschaftssystem aus Mangel an Informationen nicht mehr in der Lage ist, politische und administrative Entscheidungen zu kritisieren, ist eine der Grundlagen einer offenen Gesellschaft in Frage gestellt. Diese Schlußfolgerungen münden unmittelbar ein in die Güterabwägung auf Verfassungsebene, die einer Feststellung des öffentlichen Interesses an einer Gruppenauskunft aus dem Melderegister für Zwecke wissenschaftlicher Forschung vorausgehen muß. Die Integrität des Bürgers im Sinne von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist der wesentliche Anknüpfungspunkt für das Datenschutzrecht in seiner heutigen Konzeption. Jedoch unterliegt auch dieses Grundrecht dem Prinzip der Einheit der Verfassung. Anders gesagt, das verfassungsrechtlich verankerte allgemeine Persönlichkeitsrecht des Bürgers darf nicht zu einer Aushöhlung von grundrechtlich verbürgten Informationsrechten führen. Beide, Persönlichkeitsrecht und Wissenschaftsfreiheit, müssen vielmehr gegeneinander abgewogen werden. Mit einer solchen Abwägung ist eine untere staatliche Verwaltungseinheit in der Regel überfordert. Klare Weisungen des poli-

tisch verantwortlichen Innenministers sind hier unabdingbar. Darüber hinaus hielt ich es für denkbar, daß diese Entscheidungen, wie in der Regelung des § 16 a Abs. 2 für einen anderen Tatbestand ohnehin bereits vorgesehen, vom Innenminister als politisch verantwortlicher Instanz selbst getroffen werden. Ein derartiges Verfahren könnte dazu beitragen, die erforderliche Rechtssicherheit für die Entscheidung über den Datenzugang für wissenschaftliche Forschung herzustellen. Zugleich ist meines Erachtens allein diese Instanz auch mit dem Sachwissen ausgestattet, legitime Informationsinteressen der Wissenschaft mit dem allgemeinen Persönlichkeitsrecht des Bürgers im Sinne eines gesellschaftlichen Informationsgleichgewichts in Einklang zu bringen. Datenschutz darf nicht, wie in der Vergangenheit häufiger beobachtet, zum Behördenschutzargument gegenüber unbequemer wissenschaftlicher Forschung verkommen. Dies wäre Datenschutz in sein Gegenteil verkehrt. Derartige Tendenzen haben in den Vereinigten Staaten komplementär zu Entwicklungen des Privacy Act zur legislativen Absicherung der Informationsfreiheit im „Freedom of Information Act“ geführt. Es ist nicht auszuschließen, daß eine ähnliche Entwicklung in der Bundesrepublik zu einer gesetzlichen Absicherung der Informationsfreiheit führen muß, dies um so mehr dann, wenn die Anwendung des Datenschutzrechts die vorhandenen Erscheinungen des staatsbürgerlichen Privatismus verstärkt, statt die Einbindung des Persönlichkeitsrecht in eine Informationsstruktur, die wesentlich durch Kommunikationsgrundrechte wie Art. 5, Art. 8, Art. 9 geprägt ist, zu reflektieren. Datenschutz muß also, richtig verstanden, neben dem Schutz der persönlichen Integrität des Bürgers immer und zugleich den gesellschaftlichen Verteilungsaspekt von Informationen beachten.

Eine Lanze für die Informationsfreiheit als bisher wenig beachteten externen Effekt des Datenschutzes zugunsten wissenschaftlicher Forschung zu brechen, heißt andererseits nicht, daß Wissenschaft und Forschung datenschutzimmun sind. Wissenschaftliche Forschung muß sich im Rahmen der verfassungsmäßigen Rechtsordnung bewegen, also: Datenschutzrecht begrenzt wissenschaftliche Forschung, die den Menschen zum Gegenstand hat, d. h., verlangt wird der Respekt vor der Integrität des Bürgers als formale institutionelle Rahmenbedingung von Wissenschaft überhaupt. Darüber hinaus stellt das Datenschutzgesetz keine materiellen Kriterien für

Forschung auf. Ausdruck dieses formalen Rahmens ist die Zulässigkeit der Datenverarbeitung mit Einwilligung des Betroffenen, oder wenn nach Art der Daten ihrer Verwendung oder ihrer Offenkundigkeit kein Anlaß zu der Annahme besteht, daß schutzwürdige Belange von Betroffenen beeinträchtigt werden. Selbstverständlich ist, daß eine Datenverarbeitung im Wissenschaftssystem nicht zu Maßnahmen gegen den Betroffenen führen darf. Bei personenbezogenen Daten, die für wissenschaftliche Zwecke gegeben werden, muß gewährleistet sein, daß der Informationsstrom bei der Forschungseinrichtung endet, also gewissermaßen in eine Sackgasse mündet: Der Betroffene soll sicher sein können, daß seine personenbezogenen Daten nur für ein bestimmtes Forschungsprojekt verarbeitet werden und nur mit seiner Einwilligung weiter übermittelt werden dürfen. Es muß ganz und gar ausgeschlossen sein, daß aus wissenschaftlichen Befragungen Maßnahmen gegen den Betroffenen ergriffen werden, mit anderen Worten, daß sich wissenschaftliche Daten zu Interventionsdaten verwandeln. Besondere Aufmerksamkeit verdienen in diesem Zusammenhang die Fragen der Einwilligung von Betroffenen und die Information über den Zweck und das Ziel des Forschungsvorhabens, deren besondere Bedeutung sich in dem Aufbau epidemiologischer Krankheitsregister, wie z. B. Krebsregister, aufzeigen läßt. Epidemiologie sei hier definiert als Wissenschaft, die die Verteilung von Krankheiten bei Menschen und ihre Determinanten untersucht. Ein Krebsregister z. B. umfaßt alle Daten eines Krebspatienten von der ersten Diagnosestellung an über den weiteren Krankheitsverlauf und externer Variablen, wie z. B. Umwelteinflüsse, Arbeit in einem Asbestwerk, regionale Mobilität usw. bis zur Todesbescheinigung. Der Personenbezug muß, damit der Forschungszweck nicht vereitelt wird, aufrecht erhalten werden, um den Verlauf der Krankheit und äußere Determinanten unter Umständen über Jahrzehnte hinweg verfolgen zu können. Ein anonymisiert geführtes Register wäre sinnlos, da es aufgrund der Gefahr von Doppelmeldungen weder eine exakte Zahl der Patienten zu einem Zeitpunkt, noch eine Schätzung der Neuerkrankungsrate für einen bestimmten Zeitraum zuläßt. Eine Einwilligung der Patienten kann bei Krebs z. B. in Folge einer Aufklärung über die tatsächliche Diagnose den Therapieerfolg in einem erheblichen Prozentsatz schwer gefährden. Zum anderen reicht bei einer Speicherung, die sich unter

Umständen über Jahrzehnte erstrecken, eine einmalige Einwilligung nicht aus, zumal sich die Daten der einzelnen Patienten im Zeitverlauf erheblich verändern können. Allein die Frage, wie bei einer Langzeitspeicherung personenbezogener Daten in einem Krankheitsregister die Rechte des Betroffenen, wie Auskunft, Berichtigung, Sperrung und Löschung aktualisiert werden können, ist nach gegenwärtigem Rechtszustand nur schwer zufriedenstellend zu lösen. Im Falle des Krebsregisters, dessen Bedeutung für das überragende Gemeinschaftsgut der Volksgesundheit in diesem Zusammenhang noch einmal unterstrichen werden soll, wird sachlich die Totalität aller Krebsfälle erfaßt und verarbeitet. Auch eine die wissenschaftliche Forschung privilegierende Lösung, wie die des § 15 Hessisches Datenschutzgesetz, reicht als Legitimationsgrundlage für eine derartige Verarbeitung personenbezogener Daten nicht aus. Hier ist der Gesetzgeber gefordert, eine gesetzliche Grundlage für ein Krebsregister zu schaffen und dieses Gesetz mit bereichsspezifischen Datenschutzregelungen zu versehen, die der Sensitivität der gespeicherten Daten angemessen sind.

2.1.8 Auftragsforschung

Ein in der Praxis immer wieder beobachtetes Phänomen ist die Auftragsforschung durch öffentlich-rechtliche oder private Forschungsinstitute für die öffentliche Verwaltung. Die Untersuchungen dienen ganz unterschiedlichen Zwecken, auf der Ebene der Ressorts z. B. der Vorbereitung von Fachplanung und Gesetzentwürfen oder bei unteren staatlichen Verwaltungsbehörden und Kommunen meistens der Vorbereitung von raum- und regionalplanerischen Maßnahmen. Hier tritt immer wieder die Schwierigkeit für den Auftraggeber in der Beurteilung der datenschutzrechtlichen Verantwortung und der Vertragsgestaltung auf, die in der Vergangenheit wiederholt zu Interventionen des Hessischen Datenschutzbeauftragten geführt hat.

So beauftragte z. B. eine mittelhessische Großstadt ein namhaftes privates Institut für Stadtplanung mit einer Untersuchung der Verkehrs- und Wohnsituation der Stadt. Der Oberbürgermeister bat mich um Stellungnahme zu der Frage, unter welchen Voraussetzungen Einwohnerdaten aus Dateien der Stadt an das Institut übermittelt werden dürfen. Nach Abschluß der Untersuchung stellte sich heraus, daß dieses von der Stadt mit der Untersuchung beauftragte Institut seinerseits

ein Marktforschungsunternehmen als Subunternehmen für die Durchführung der im Rahmen der Untersuchung notwendigen Interviews vertraglich verpflichtet hatte. Welche Institution hier speichernde Stelle war und damit verantwortlich für Maßnahmen des Datenschutzes, war der Gesetzeslage in der Tat nicht so einfach zu entnehmen. Diese Frage ist auch in den verbreiteten Kommentierungen nach wie vor strittig. Der Hessische Datenschutzbeauftragte sah sich vor die Frage gestellt, ob der Sachverhalt nach den Regelungen für die unabhängige wissenschaftliche Forschung (§ 15 HDSG) oder der Auftragsdatenverarbeitung zu lösen sei. Er hat sich für eine entsprechende Anwendung der Regelung über die Auftragsverarbeitung entschieden. Dabei standen folgenden Überlegungen im Vordergrund:

Der Bürger muß wissen, wer zu welchem Zweck Daten von ihm erhebt, und wie sie verarbeitet und verwertet werden. Eine Untersuchung mit einer klaren administrativen Hilfsfunktion, die zudem noch nach außen als „Befragung nach Wohnungs- und Verkehrssituation der Stadt“ durch den Oberbürgermeister der Stadt angekündigt war, mußte im Ergebnis auch zur datenschutzrechtlichen Verantwortung der Stadt führen. Obwohl man bei der materiell-rechtlichen Prüfung Zweifel daran hegen kann, ob diese Datenverarbeitung im Rahmen der wissenschaftlichen Forschung wegen der Gestaltungsfreiheit des Untersuchungsdesigns Auftragsverarbeitung ist, die nur aufgrund bindender Weisung des Auftraggebers erfolgen kann, war für meine Entscheidung die Durchsichtigkeit des Verfahrens und die Verantwortungsklarheit entscheidend. Ich habe daher angeregt, vertraglich zu sichern, daß der Auftragnehmer im Rahmen des Werkvertrages sich den Bestimmungen des Hessischen Datenschutzgesetzes und der Aufsicht des Hessischen Datenschutzbeauftragten zu unterwerfen hat. Die Folge ist, daß die Stadt speichernde Stelle bleibt und das Institut nur nach Weisungen verfahren kann. Ein solches Verfahren ist allgemein dann angebracht, wenn sich Behörden und öffentliche Stellen wissenschaftlicher Untersuchungen zur Erfüllung planerischer Aufgaben oder Vorbereitung von administrativen Erhebungen bedienen. Weisung kann hier semantisch nicht auf die Bedeutung der Einzelweisung reduziert werden.

Vielmehr hat sich jede öffentliche Stelle ein vollständiges Forschungsdesign durch das Institut als Vertragspartner vorlegen zu lassen.

Dieses Forschungsdesign wird dann zum Gegenstand des Vertrages selbst. Änderungen des Forschungsdesigns, die die Verarbeitung personenbezogener Daten betreffen, sind als Vertragsänderungen zu behandeln, denen der öffentliche Auftraggeber ausdrücklich zustimmen muß. Die Unterwerfung des Auftragnehmers unter die Regelungen des Hessischen Datenschutzgesetzes und die Aufsicht des Hessischen Datenschutzbeauftragten sind gleichfalls im Vertrag sicherzustellen. Durch eine solche Konstruktion wird erreicht, daß jede durch Dritte ausgeführte wissenschaftliche Befragung mit administrativer Hilfsfunktion Auftragsverarbeitung im Sinne des Hessischen Datenschutzgesetzes ist. Ich füge jedoch hinzu, daß eine Rechtsnorm, die die Datenverarbeitung für planerische und statistische Zwecke von Verwaltungsbehörden regelt, nach wie vor von mir für erforderlich gehalten wird.

2.1.9 Fälle aus dem Bereich Forschung und Datenschutz

2.1.9.1 Eurocat (European Communities Concerted Action Project Registration of Congenital Abnormalities and Twins)

Am 13. Februar 1978 faßte der Rat der Europäischen Gemeinschaften einen Beschluß über eine konzertierte Aktion zur Registrierung angeborener Abnormitäten und Mehrlingsschwangerschaften. Die Mitgliedsstaaten haben sich in diesem Beschluß verpflichtet, die Errichtung von Registern und die Forschungsarbeiten im Rahmen der einzelstaatlichen Regelungen und Verfahren durchzuführen. Hauptziel der Forschungsarbeit dieses Projekts ist die Sammlung wissenschaftlicher und technischer Kenntnisse auf diesem Gebiet, das wegen seiner Bedeutung durch den Ministerrat ausgewählt worden ist. Die Forschungsaufgaben umfassen folgende Themen:

1. Registrierung angeborener Mißbildung und vererbter biochemischer und Chromosomenabnormitäten in ausgewählten Regionen der Gemeinschaft. Die Registrierung umfaßt nacheinander die Abnormitäten des Zentralnervensystems (z. B. Anencephalie und Spina bifida), das Downsyndrom, schwerwiegende Mißbildungen der Gliedmaßen, multiple Abnormitäten usw.
2. Die Registrierung von Zwillings- und Mehrlingsschwangerschaften in ausgewählten Regionen der Gemeinschaft.

3. Methodische Untersuchungen im Hinblick auf eine optimale Koordinierung, sowohl der vorhandenen nationalen Register als auch der Registrierverfahren. Die Koordinierung umfaßt für die Bundesrepublik Deutschland die in Hessen eingerichteten regionalen Register.

Dieses Register soll bei der Universität Frankfurt im Institut für Humangenetik eingerichtet werden. Das Register selbst beruht auf freiwilliger Kooperation der Geburtshelfer, Pädiater, Pathologen und der Eltern. Die Daten des lokalen hessischen Registers sollen mit einer Identitätsnummer, die lediglich den Namen ersetzt, an das Zentralregister an der Universität Löwen in Belgien übermittelt werden. Die Zuordnung des Identifikators zu Name und Adresse des Kindes bzw. seiner engeren Verwandten sind nur im lokalen Register gespeichert. Die einzelnen Falldaten werden stapelweise (in „batches“) durch die Post an Eurocat in der epidemiologischen Abteilung der Universität Löwen übermittelt. Die hohe Sensitivität der Datenarten, die im regionalen wie im europäischen Register gespeichert werden, sowie die Dauer der Speicherung genetischer Abnormitäten in personenbezogener Form lassen es wie beim Krebsregister zweifelhaft erscheinen, ob hier die einmalige Einwilligung in die Verarbeitung personenbezogener Daten im Mißbildungsregister ausreicht, um eine ausreichende datenschutzrechtliche Legitimation genetischer Register zu erreichen. Die personenbezogene Langzeitspeicherung, die aus epidemiologischer Sicht erforderlich ist, um in „follow up“-Untersuchungen oder Longitudinalstudien den Ursachen genetischer Abnormitäten auf die Spur zu kommen, bedarf meiner Auffassung nach einer gesetzlichen Rahmenregelung für die Einrichtung von Krankheitsregistern überhaupt, damit einerseits repräsentative und gültige epidemiologische Untersuchungen durchgeführt werden können, andererseits aber, um die Voraussetzungen der Verarbeitung und Verwendung der in diesen genetischen Datenbanken gespeicherten Daten besonders restriktiv zu regeln. Die Bestimmungen der Datenschutzgesetze reichen hierfür nicht aus. Ohne gängige Vorurteile gegen genetische Untersuchungen wieder beleben zu wollen, möchte ich als datenschutzpolitische Instanz nicht versäumen, auf die mißbräuchliche Verwendung derartiger genetischer Register in der Zeit des Nationalsozialismus hinzuweisen. Die besondere historische Verantwortung darf zwar nicht dazu führen, daß notwendige Forschungen, weil sie

einmal mißbraucht worden sind, überhaupt nicht mehr durchgeführt werden; sie dürfen aber andererseits wiederum nur stattfinden, wenn Mißbrauch nach menschlichem Ermessen ausgeschlossen ist. Besondere Probleme ergeben sich jedoch aus der Übermittlung der Daten aus dem regionalen Register an ein zentrales Register in Belgien. Dabei ist festzustellen, daß Belgien noch kein Datenschutzgesetz besitzt. Der Schutz der medizinischen Daten in diesem Register beruht daher allein auf einer freiwilligen Verpflichtung der beteiligten Mediziner, ihre standesethischen Normen über die ärztliche Schweigepflicht einzuhalten. Eine derartige Regelung ist für den Datenschutz inakzeptabel. Ich habe daher in Kooperation mit dem Bundesbeauftragten für den Datenschutz die Kommission der Europäischen Gemeinschaften um Aufklärung darüber gebeten, wie sie den Schutz personenbezogener genetischer Daten in Belgien im Rahmen eines Forschungsprojekts, dessen Träger die Gemeinschaft ist, sicherstellen will. Ohne eine ausdrückliche datenschutzrechtliche Verantwortlichkeit der Europäischen Kommission ist die Übermittlung genetischer Daten aus dem regionalen Register an Eurocat nach meiner Auffassung als rechtswidrig anzusehen.

2.1.9.2 Zahnmedizinische Forschung

Die Universitäts- und Poliklinik für Zahn-, Mund- und Kieferkrankheiten – Poliklinik für zahnärztliche Prothetik der Johannes Gutenberg-Universität Mainz – hat an einem Wiesbadener Gymnasium eine Erhebung über Ernährung und Zahngesundheit von Schulkindern durchgeführt. Die Erhebung ist vom Hessischen Kultusminister mit mehreren Auflagen genehmigt worden. Nach Durchsicht der Erhebungsunterlagen bin ich zu der Auffassung gelangt, daß in mehrfacher Hinsicht gegen das Hessische Datenschutzgesetz, den Erlaß des Hessischen Kultusministers vom 4. Mai 1977 (Amtsblatt S. 256) und sonstige Datenschutzvorschriften verstoßen worden ist. Gemäß Ziff. 2 des genannten Erlasses müssen für „Anträge auf Durchführung wissenschaftlicher Untersuchungen im Schulbereich“ neben anderen Voraussetzungen die Erhebungsunterlagen vorgelegt werden. Aus ihnen muß deutlich der Zweck der Untersuchung, die durch den Antragsteller vorgesehene Behandlung der Erhebungspapiere und deren endgültiger Verbleib hervorgehen. Im Antrag sollen Hinweise über die voraussichtliche Dauer der Datenspeicherung und den

Zeitpunkt der Löschung des Datenmaterials enthalten sein. Hierzu stelle ich fest, daß der Antrag vom Februar 1979 durch die Antragsteller zwar unterzeichnet, aber außer der Darlegung des Zwecks der Untersuchung zu den anderen Tatbestandsmerkmalen des Erlasses keine Angaben enthält. Es ist auch nicht ersichtlich, ob der Kultusminister um eine entsprechende Ergänzung des Antrags gebeten hat. Nach den Grundsätzen der §§ 7, 11 Abs. 2 HDSG und Ziff. 3, 4 des Erlasses des Hessischen Kultusministers vom 4. Mai 1977 dürfen wissenschaftliche Untersuchungen im Schulbereich nur auf freiwilliger Grundlage und mit Einwilligung der Betroffenen bzw. der Erziehungsberechtigten erfolgen. Voraussetzung für die Freiwilligkeit der Teilnahme an der Untersuchung ist eine hinreichende Aufklärung der Betroffenen über den Zweck der Untersuchung und die Verwendung ihrer Daten (sog. „informed consent“). Das Schreiben an die Eltern der betroffenen Schüler am Wiesbadener Gymnasium informiert jedoch völlig unzureichend über Zweck und Umfang der Befragung. Über die Verwendung der Daten wird keine Auskunft erteilt. Darüber hinaus ist nicht auszuschließen, daß bei den Beteiligten aufgrund des Schreibens der Eindruck entstand, es handele sich um eine Befragung im Rahmen der schulärztlichen Untersuchung. Ferner wußten die Eltern zum Zeitpunkt ihrer Einwilligung nicht, daß auf dem Erhebungsbogen nach ihren sozialstatistischen Daten und Erziehungsmethoden sowie nach Medikamentenverbrauch und sonstigen Krankheiten des Kindes gefragt werden sollte.

Es gibt daher Grund zu der Annahme, daß die Betroffenen bzw. deren Eltern keine wirksame Einwilligung zur Erhebung und Verarbeitung ihrer personenbezogenen Daten gegeben haben, da sie über Inhalt und Umfang dessen, wozu sie die Willenserklärung abgegeben haben, nicht zureichend informiert waren. Gemäß Ziff. 3 des Erlasses des Hessischen Kultusministers muß die Anonymität der zu Befragenden gewahrt sein. Von der Anonymität der Probanden der Befragung konnte überhaupt keine Rede sein. So beginnt der Erhebungsbogen mit den Fragen nach Name, Geburtsdatum, Geschlecht, Alter und Staatsangehörigkeit. Da mit der Erhebung auch noch ärztliche Untersuchungen verbunden waren, war nicht auszuschließen, daß auch die ärztliche Schweigepflicht, § 203 StGB sowie die einschlägigen Straf- und Ordnungswidrigkeitenbestimmungen des Hessischen Datenschutzgesetzes verletzt waren.

Es steht weiter fest, daß nach Auskunft der Datenschutzkommission Rheinland-Pfalz das erhebende Institut der Johannes Gutenberg-Universität sein Datenverarbeitungsvorhaben nicht angezeigt hat, wozu es nach § 10 Rheinland-Pfälzisches Datenschutzgesetz gegenüber der Datenschutzkommission verpflichtet ist. Auch hier bestehen also Zweifel, ob das Hessische Kultusministerium seine Genehmigung zur Erhebung erteilen durfte, ohne vorher zu prüfen, ob das Institut die Voraussetzung für eine rechtmäßige Datenverarbeitung im Sinne des jeweils gültigen Datenschutzgesetzes erfüllt. Darüber hinaus hätte die Genehmigung mit der Auflage verbunden werden müssen, daß in entsprechender Anwendung des § 15 Hessisches Datenschutzgesetz die Weitergabe personenbezogener Daten nur mit Einwilligung der Betroffenen zulässig ist. Die Auflage des Schreibens des Hessischen Kultusministers an die Antragsteller war unzureichend, entsprach nicht dem Bezugsverlaß des Kultusministers selbst und war obendrein mißverständlich. Es kann nicht genügen, die Antragsteller formal auf die Bestimmungen des Hessischen Datenschutzgesetzes vom 31. Januar 1978 hinzuweisen, zumal wenn bereits aus den für die Antragstellung vorgelegten Erhebungsunterlagen eindeutig ersichtlich ist, daß den Datenschutzbestimmungen bereits zum Zeitpunkt der Antragstellung nicht entsprochen worden ist. Vielmehr hätte der Antrag nur genehmigt werden dürfen, wenn aus den Erhebungsunterlagen und der Projektbeschreibung hervorgeht, daß die Bestimmungen des Hessischen Datenschutzgesetzes bereits Berücksichtigung gefunden haben.

Der Hessische Sozialminister hat, ohne Datenschutzgesichtspunkte überhaupt zu berücksichtigen, sein Einverständnis damit erklärt, daß die Erhebung über Ernährung und Zahngesundheit von behinderten Kindern im Rahmen des gleichen Forschungsprojekts in überregionalen hessischen Behinderteneinrichtungen durchgeführt wurde.

In diesem Fall haben die obersten Landesbehörden, die nach § 5 des Hessischen Datenschutzgesetzes allein für die Einhaltung des Datenschutzes in ihrem Geschäftsbereich verantwortlich sind, einmal ohne Berücksichtigung des Datenschutzgesetzes überhaupt gehandelt, im anderen Falle trotz optimaler Handlungsanweisungen durch einen – in Zusammenarbeit mit mir entstandenen – Erlaß den Datenschutz verletzt. Der Vorfall erweist erneut, daß die Unsicherheit in der

Anwendung des geltenden Datenschutzrechts bei allen Behörden wesentlich mehr verbreitet ist, als man annimmt. Ich habe daher Gespräche sowohl mit dem Hessischen Sozialminister wie mit dem Hessischen Kultusminister aufgenommen, um den bisherigen Mängeln in der Anwendung des Datenschutzrechts in Zukunft wirksam abhelfen zu können.

2.2 Transparenz der Datenverarbeitung

2.2.1 Erhebung von Daten beim Betroffenen

Sofern die Behörde beim Betroffenen direkt Daten erheben will, hat sie ihn auf die Rechtsvorschrift hinzuweisen, die diese Erhebung gestattet. Liegt der Erhebung keine Rechtsvorschrift zugrunde, ist der Betroffene auf die Freiwilligkeit seiner Angaben hinzuweisen. Es dürfen ihm außerdem aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen (§ 11 Abs. 2 HDSG).

Was bedeutet diese Vorschrift in der Praxis?

Die „Erhebung“ von Daten erfolgt meist in der Weise, daß der Bürger (Betroffener) von der Verwaltung aufgefordert wird, ein Antragsformular auszufüllen. Für die Behörde ist nun seit Inkrafttreten des Hessischen Datenschutzgesetzes insofern eine neue Situation entstanden, als diese „Anträge“ oder „Erhebungsbogen“ auf die Formvorschrift des § 11 Abs. 2 HDSG hin zu überprüfen sind. Das heißt, die Rechtsgrundlage der Erhebung (spezialgesetzliche Vorschrift, § 11 Abs. 1 HDSG oder Einwilligung des Betroffenen) ist auf dem Vordruck anzugeben. Meine Erfahrungen haben gezeigt, daß in einer Vielzahl von Fällen die herangezogene Rechtsgrundlage – z. B. eine spezialgesetzliche Regelung – nicht alle gestellten Fragen abdeckt, sondern für bestimmte Fragen auf die Freiwilligkeit des Betroffenen hinzuweisen ist.

Ein weiterer Gesichtspunkt ist die Rechtsgrundlage für die Verarbeitung der erhobenen Daten. § 7 HDSG führt hierzu aus, daß die Verarbeitung personenbezogener Daten (Speicherung, Übermittlung, Veränderung und Löschung), die von dem HDSG geschützt werden, nur zulässig ist, wenn das HDSG oder ein anderes Gesetz (spezialgesetzliche Regelung) sie erlaubt oder der Betroffene eingewilligt hat. Ich habe festgestellt, daß gerade im Bereich der Übermittlung personenbezogener Daten es oft an einer gesetzlichen Grundlage fehlt und deshalb die Einwilligung des Betroffenen herbeigeführt werden muß. Bei der

Änderung und Neugestaltung von Vordrucken sollte deshalb in visuell herausragender Weise (Druck in Kursivschrift, halbfett oder Umrahmung des Textes) die Erfordernisse des § 11 HDSG (Hinweis auf die Rechtsgrundlage der Erhebung) und die des § 7 HDSG (Einwilligung des Betroffenen) erfüllt werden.

Als Beispiel für eine gute Lösung ist hier der in Zusammenarbeit mit dem Hessischen Minister für Wirtschaft und Technik entstandene Vordruck für die Zulassung eines Kraftfahrzeugs zu erwähnen oder der in Zusammenarbeit mit dem Minister für Landesentwicklung, Umwelt, Landwirtschaft und Forsten entstandene Vordruck auf Gasölverbilligung für landwirtschaftliche Betriebe. Ein negatives Beispiel besonderer Art ist das Formular zur An-, Ab- bzw. Ummeldung nach dem Hessischen Meldegesetz. Mit diesem durch Verwaltungsvorschrift landeseinheitlich gestalteten Vordruck werden bei dem Bürger eine Vielzahl von Daten nach Vorschriften des Melderechts, Wahlrechts und Steuerrechts erhoben und übermittelt. Der Vordruck enthält jedoch keine Hinweise nach § 11 HDSG.

Der Hessische Minister des Innern ist meiner Anregung, diesen Vordruck umzugestalten, unter Hinweis auf den zur Zeit in Beratung befindlichen Entwurf eines Bundesmelde-rechtsrahmengesetzes leider nicht gefolgt.

2.2.2 Dateienregister

2.2.2.1 Stand des Verfahrens

§ 25 Abs. 1 HDSG enthält die Vorschrift, beim Hessischen Datenschutzbeauftragten ein Register der Dateien zu führen, in denen personenbezogene Daten gespeichert werden. Die Einzelheiten des Meldeverfahrens hat die Landesregierung in der unter meiner Mitwirkung entstandenen Hessischen Datenschutzregisterordnung²⁾ geregelt. Erfahrungen mit einem aufgrund eines Kabinettsbeschlusses der Hessischen Landesregierung vom 6. Juli 1971 geführten manuellen Dateienregister und der sich abzeichnende Umfang der zu registrierenden Dateien haben mich veranlaßt, von Anfang an eine ADV-unterstützte Lösung dieses Problems anzustreben. Das von meiner Dienststelle entwickelte Konzept „Führung und Auswertung des Dateienregisters beim Hessischen Datenschutzbeauftragten“, bei

²⁾ Hessische Verordnung über die von dem Hessischen Datenschutzbeauftragten zu führenden Dateienregister (Hess. Datenschutzregisterordnung – HDSRegO – vom 8. Dezember 1978, GVBl. I, S. 682).

dem die Kanzlei des Hessischen Landtags und die HZD technische Hilfestellung leisteten, sieht den Einsatz eines bereits vorhandenen Standard-Dokumentationsprogramms (LE-DOC) vor. Als erforderliche technische Einrichtung soll eine mit der HZD durch Standleitung verbundene Datenstation in meiner Dienststelle installiert werden. Erstellung und Führung des Dateienregisters – einschließlich der erforderlichen Auskunftserteilung – sollen durch dieses Terminal erfolgen. Die erforderlichen Haushaltsmittel sind im Entwurf des Haushaltsplans 1980 eingeplant, der Bericht über die Verfahrenskonzeption durch den Landesautomationsausschuß verabschiedet.

Wie ich bereits erwähnte, gibt es beim Aufbau des Dateienregisters zahlreiche Schwierigkeiten. Außer der unzureichenden Personal- und Sachausstattung meiner Dienststelle liegen diese besonders im organisatorischen Bereich. So ist gerade bei den kreisangehörigen Gemeinden und den sonstigen der Aufsicht des Landes unterstehenden Stellen der Wissensstand über die Regelungen der HDSRegO sehr gering. Die Folge davon sind unzählige telefonische Anfragen bei meiner Dienststelle und umfangreicher Schriftverkehr mit den meldepflichtigen Stellen. Hier fehlt es nach meinen Erfahrungen an einer zielgerichteten Information durch die Aufsichtsbehörden, um die Regelungen des HDSG – soweit sie das Dateienregister betreffen – und die Zielsetzung der HDSRegO für die betroffenen Stellen verständlich zu machen.

2.2.2.2 Stand der Meldungen zum Dateienregister

Gemäß § 3 der HDSRegO waren bestehende Dateien innerhalb eines halben Jahres nach Inkrafttreten der Verordnung zu melden. Diese Frist war am 9. Juni 1979 abgelaufen. Bis Ende November 1979 hatten rund 3 000 speichernde Stellen (75% des geschätzten Bestandes) etwa 8 000 Dateien (25%) zum Register angemeldet. Die Meldungen werden zur Zeit auf ihre Richtigkeit und Vollständigkeit hin überprüft.

Bereits jetzt kann gesagt werden, daß Umfang und Qualität der erstatteten Meldungen stark voneinander abweichen. Die Meldungen der kreisfreien Städte differieren zwischen 23 gemeldeten Dateien als Minimum und 57 Dateien als Maximum. Nur eine kreisfreie Stadt des Landes hatte bis Ende November trotz mehrfacher Erinnerung noch keine einzige Datei zum Dateienregister gemeldet. Ein ähnliches Bild zeigt sich bei den Meldun-

gen der Landkreise bzw. kreisangehörigen Gemeinden. Während ein Landkreis in einer sehr ausführlichen und sorgfältig aufbereiteten Zusammenstellung die Einzelmeldungen von 91% seiner Gemeinden zusammengefaßt hatte, umfaßte die Meldung eines anderen Kreises ganze 13% der kreisangehörigen Gemeinden. Noch keine Übersicht liegt über die Meldungen der speichernden Stellen der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen vor. Diese meldepflichtigen Stellen erscheinen auch am schwierigsten zu erfassen, da mir keine Aufstellungen dieser Adressaten vorliegen und somit langwierige Recherchen erforderlich sind.

2.2.2.3 Fehlerhafte Meldungen

Eine erste Auswertung der in meiner Dienststelle vorliegenden Meldungen hat ergeben, daß der weitaus größte Teil formale und inhaltliche Fehler aufweist. So ist insbesondere zu beanstanden:

1. Der Inhalt der Hessischen Datenschutzregisterordnung ist hauptsächlich kleineren speichernden Stellen nicht bekannt.
2. Der vorgeschriebene Meldeweg wird nicht eingehalten.
3. Der als Bestandteil der Hessischen Datenschutzregisterordnung beigefügte Meldevordruck wird nicht verwendet.
4. Der Vordruck wird unvollständig ausgefüllt.
5. Es werden Durchschriften von Veröffentlichungen nach der Hessischen Datenschutzveröffentlichungsordnung als Meldung zum Dateienregister angesehen.
6. Aufsichtsbehörden leiten die Meldungen der kreisfreien Gemeinden ohne Vorprüfung weiter.
7. Es besteht große Unklarheit darüber, welche Dateien zu melden sind. So hat eine Gemeinde den Haushaltsplan zum Dateienregister gemeldet, eine Reihe anderer Gemeinden das Einwohnerregister nicht als Datei angesehen.
8. Unklarheit besteht nach wie vor bei der Abgrenzung von Dateien, die manuell geführt werden und nicht zur Übermittlung bestimmt sind (interne Dateien).

Im großen und ganzen bewährt hat sich das Einschalten der Verbundrechenzentren bei der Meldung der landeseinheitlichen ADV-Verfahren. Dadurch, daß den spei-

chernden Stellen wesentliche Teile der Meldung, wie z. B. die Dateiinhalte, vorgegeben waren, ist die Fehlerquote in diesen Meldungen sehr gering.

2.2.2.4 Künftige Aufgabenstellung

Das Dateienregister wird nach Fertigstellung nicht nur ein Organisationsmittel sein, das es dem Datenschutzbeauftragten ermöglichen wird, seinen Prüfungs- und Überwachungsaufgaben nachzukommen, sondern auch eine wesentliche Rolle bei der Verwirklichung der dem Bürger durch das Hessische Datenschutzgesetz eingeräumten Rechte spielen. Die seit Inkrafttreten des Gesetzes erfolgten Dateiveröffentlichungen von speichernden Stellen haben ihren Zweck, die Datenverarbeitung im öffentlichen Bereich für den Bürger transparenter zu machen, nicht erfüllt. Die Gründe hierfür sind einmal darin zu suchen, daß die Veröffentlichungen zum Teil in speziellen Medien – wie dem Staatsanzeiger des Landes Hessen – erfolgten, die nur wenigen Bürgern zugänglich sind und zum anderen in der bisweilen doch recht mangelhaften Aussagekraft der Veröffentlichungstexte bestehen.

Um so mehr Aufmerksamkeit sollte einem gut funktionierenden Dateienregister gewidmet werden. Dieses könnte uns dem Ziel der größeren Transparenz der ADV ein Stück näher bringen.

2.2.3 Unterrichtung und Beratung über Datenschutz – Zusammenarbeit mit Datenschutz-Aufsichtsbehörden – Beteiligung an Lehrveranstaltungen

Meine Inanspruchnahme auf dem Gebiet der Information über Datenschutz, der Beratung von Behörden und anderen Stellen sowie für den Erfahrungsaustausch mit anderen Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz hat im vergangenen Jahr ganz beträchtlich zugenommen, alles in allem um ca. 60%. Dem entspricht die erheblich vermehrte Zahl von Bürgerbeschwerden, Bitten um Auskunft oder um Übersendung von Informationsmaterial. Auch meine Beteiligung an Informationsveranstaltungen über Datenschutz von Behörden und öffentlich-rechtlichen Körperschaften hat sich gegenüber dem Vorjahr weiter erhöht.

Von meinem Faltblatt „Datenschutz ist Bürgerschutz“ wurden, teils über Schulen und Verwaltungen, teils auf Anforderung von Bürgern in diesem Jahr ca. 120 000 Exemplare verteilt.

An einfachen telefonischen oder mündlichen Anfragen von Bürgern erreichen mich monatlich ca. 1 000. Dabei handelt es sich um allgemeine Anfragen über das Hessische oder das Bundesdatenschutzgesetz, insbesondere die darin enthaltenen Rechte des Bürgers. Auch die Zahl der schriftlichen Bürgerbeschwerden wegen unzulässiger Datenverarbeitung, die auf konkrete Fälle zurückzuführen sind, hat sich im abgelaufenen Jahr erheblich erhöht. 70 Bürgerbeschwerden haben zu Beanstandungen wegen Datenschutzmängeln bei Behörden geführt. Die meisten davon konnten inzwischen abschließend bearbeitet werden; mehrere davon führten zu Empfehlungen an die zuständige Fachbehörde, ihr Verfahren zu ändern. Beispiele solcher Empfehlungen enthält dieser Bericht.

Auch die Zahl der Anfragen und Bitten um Beratung von Behörden steigt ständig. Es handelt sich dabei um Behörden und öffentliche Stellen der verschiedensten Aufgabebereiche, angefangen vom Staatsarchiv, über Bergamt, Hochschulen, Krankenhäuser, Landwirtschaftsverwaltung, Ministerien, Polizei, Rechenzentren, Schulen, Stadtverwaltungen bis hin zu wissenschaftlichen Institutionen. Bei mindestens 70 Anlässen erwies sich eine ausführliche Beratung mit mindestens einer, oft aber mehreren, mehrstündigen Besprechungen als notwendig, um die besonderen Datenschutzprobleme eines EDV-Projekts, eines geplanten Gesetzes oder eines behördlichen Verfahrens zu erkennen und Lösungsvorschläge gemeinsam vorzubereiten. Daneben sind der Hessische Datenschutzbeauftragte wie auch seine Mitarbeiter in zahlreichen Fällen mündlich und telefonisch von Behörden um Rat gefragt worden. Fast immer konnte durch eine frühzeitige Beratung über Datenschutz erreicht werden, daß bei der Automatisierung bisher manuell durchgeführter Verwaltungsaufgaben Probleme vermieden wurden, wie sie bei dem Versuch, Datenschutz nachträglich in fertige Verfahren einzuführen, die Regel sind.

Ein ausführlicher Erfahrungsaustausch mit einer großen Zahl von Fachbehörden auf Landes- wie auch Kommunalebene sowie mit dem Bundesbeauftragten für den Datenschutz und den anderen Landesbeauftragten war Voraussetzung dafür, diese fachliche Beratung erfolgreich führen zu können. 31 Zusammenkünfte im vergangenen Jahr dienten diesem Zweck.

Auf mehreren Ebenen gibt es inzwischen einen regelmäßigen Erfahrungsaustausch. So

wurde auf meine Anregung hin erstmals eine Konferenz der Datenschutzbeauftragten der Bundesländer – an der sich auch der Bundesbeauftragte für den Datenschutz beteiligt – einberufen. Diese Zusammenkünfte werden inzwischen regelmäßig fortgesetzt und haben sich als wertvolle Möglichkeit erwiesen, die Datenschutzpraxis im Bereich der öffentlichen Verwaltung der Länder und des Bundes im Interesse des Bürgers einheitlich zu gestalten.

Auch ein Erfahrungsaustausch über Datenschutzprobleme im kommunalen Bereich zwischen den hessischen Großstädten und großen kreisangehörigen Städten sowie den Datenschutz-Aufsichtsbehörden (HMdI, HDSB) ist auf meine Initiative als regelmäßige Einrichtung vereinbart worden; er hat inzwischen nützliche Impulse für die Handhabung des Datenschutzes durch die Stadtverwaltungen und zur Koordinierung von einschlägigen Maßnahmen bewirkt.

Dieses Anwachsen der Aufgaben – insbesondere auf dem Gebiet der Beratung von Behörden und öffentlichen Stellen – droht, das Gleichgewicht der Tätigkeiten meiner Dienststelle in Frage zu stellen: Diese Beratung geht zwangsläufig zu Lasten einer raschen Bearbeitung von Bürgereingaben sowie des Umfangs meiner Kontrolltätigkeit, vor allem im Bereich der Datensicherung.

Die immer noch vielfach anzutreffende Unsicherheit über die Anwendung des Hessischen Datenschutzgesetzes und der übrigen Datenschutzbestimmungen durch Behörden läßt nach wie vor die Ausbildung auf dem Gebiet des Datenschutzes als eine dringliche Aufgabe erscheinen. Aus diesem Grunde habe ich selbst in einer größeren Zahl von Vorträgen, Rundfunksendungen und Veröffentlichungen Verständnis für die Notwendigkeit und die Probleme des Datenschutzes zu wecken versucht. Meine Mitarbeiter haben darüber hinaus weitere Vorträge und Referate zu Fachfragen des Datenschutzes gehalten. Bereits viermal habe ich dem Landespersonalamt Hessen für mehrtägige Einführungsseminare in den Datenschutz für Angehörige der Landes- und Kommunalverwaltung Mitarbeiter als Dozenten und als Seminarleiter zur Verfügung gestellt.

Angesichts der bereits genannten Zahl von 3 000 speichernden Stellen allein in der öffentlichen Verwaltung des Landes Hessen können diese Bemühungen um bessere Unterrichtung über den Datenschutz jedoch nach wie vor nicht als ausreichend angesehen werden. Im

Hinblick auf die stark gewachsene Beanspruchung meiner Mitarbeiter für laufende Aufgaben der Datenschutzüberwachung wird die Beteiligung an Informations- und Lehrveranstaltungen zunehmend schwieriger. Ich empfehle daher dringend, von seiten der beteiligten Verwaltungen selbst eine hinreichende Zahl solcher Veranstaltungen für Verwaltungsbedienstete durchzuführen. § 5 HDSG betont ausdrücklich, daß die Behörden jeweils für ihren Bereich für die Beachtung der Datenschutzbestimmungen verantwortlich sind. Diese Verantwortung kann ihnen weder meine Mithilfe bei Informationsveranstaltungen noch meine Aufsicht über die Einhaltung des Hessischen Datenschutzgesetzes abnehmen.

2.3 Entwicklung bei den Sicherheitsbehörden

2.3.1 Kriminalpolizeiliche Sammlungen (KpS)

Die Innenministerkonferenz hat durch ihren Arbeitskreis II-Beschluß vom 28./29. März 1979 einen Musterentwurf über Richtlinien für die Führung kriminalpolizeilicher Sammlungen vorgelegt. Mit Wirkung vom 15. Mai 1979 wurde dieser vom Arbeitskreis II empfohlene Musterentwurf für das Bundeskriminalamt vorläufig in Kraft gesetzt. Diese Richtlinie regelt das Sammeln, Aufbewahren und die Aussonderung von kriminalpolizeilichen Informationsbeständen ebenso wie die Auskunftserteilung. Zweck der KpS-Richtlinien ist unter anderem, den Forderungen des Datenschutzes entgegenzukommen und entsprechend dem Gebot der Verhältnismäßigkeit polizeilichen Handelns die Dauer der Aufbewahrung personenbezogener Unterlagen zeitlich in klarer Weise zu begrenzen. Ich habe mich bereits zu einem frühen Zeitpunkt zu den ersten Entwürfen der KpS geäußert und sie als einen bedeutsamen Schritt im Hinblick auf die Verwirklichung des Datenschutzes und einer Verrechtlichung des Informationsverhaltens der Polizei begrüßt.

Die intensiven Diskussionen, die Stellungnahmen der Datenschutzbeauftragten der Länder und des Bundes haben eine Reihe neuer Gesichtspunkte erbracht, die die Arbeitsgemeinschaft Kripo, einen Arbeitskreis der Leiter der Landeskriminalämter, veranlaßt hat, eine Arbeitsgruppe Fahndung einzusetzen mit der Aufgabe, zu dem vom Arbeitskreis II empfohlenen Musterentwurf nicht nur ergänzende Vorschläge zu unterbreiten, sondern ihn auch materiell zu ändern. Die

wichtigsten materiellen Änderungen aus der Sicht des Datenschutzes sind

- eine präzisierte Regelung der Zugriffskontrolle sowie der Benutzerkontrolle (KpS 5.3)
- eine neue Regelung der Auskunft an den Betroffenen (KpS 6)
- die Bestimmung über die regelmäßige Aussonderung (KpS 8.3), die Verkürzung der Prüflisten für die Aussonderung bei Bagatelldelikten (Ziff. 8.3.3)
- die Prüfliste bei der Speicherung von Kindern und Jugendlichen (Ziff. 8.3.5).

Der erneut von der AG Fahndung erarbeitete und von der AG Kripo vorgelegte Entwurf der KpS weist eine Anzahl von Verbesserungen datenschutzrechtlicher Art auf, z. B. im Bereich der Auskunft an den Betroffenen und bei den Voraussetzungen für die weitere Aufbewahrung bei Kindern und Jugendlichen und verkürzte Aufbewahrungsfristen der KpS bei Bagatelldelikten.

In Gesprächen mit Vertretern des LKA und des Hessischen Ministers des Innern konnten konkrete Verbesserungsvorschläge zur Zugriffsregelung zur Auskunft an den Betroffenen und zur Speicherung von Bagatelldelikten erreicht werden. Allerdings bestehen nach wie vor grundsätzliche Meinungsverschiedenheiten über die Speicherung von Kindern und Jugendlichen und die damit zusammenhängenden Aussonderungsbestimmungen.

2.3.2 Speicherung von Daten über Kinder in Polizei-Informationssystemen

Obwohl ich angesichts der zunehmenden Kinderdelinquenz in großstädtischen Ballungsgebieten, die sich nicht nur auf Bagatelldelikte erstreckt, die Aufgabe der Sicherheitsbehörden nicht verkenne, muß man sich davor hüten, dieses abweichende Verhalten nur als polizeiliches Problem zu beschreiben. Neben der Aufgabe der Gefahrenabwehr sind auch und gerade spezialpräventive Maßnahmen vordringlich, die von anderen Instanzen sozialer Kontrolle getroffen werden müssen als von der Kriminalpolizei. Die Tatsache, daß jeder Ladendiebstahl, jede „Schwarzfahrt“ (sog. Beförderungerschleichung) – im Grunde also diejenigen Delikte, die in der hochindustriellen Gesellschaft das „Äpfelklauen“ abgelöst haben – in einer polizeilichen Akte oder Datei festgehalten werden, ist höchst bedenklich. Hier soll keineswegs bestritten werden, daß die genannten Delikte auch den Beginn krimineller Karrieren von

Kindern darstellen können; andererseits ist aber abweichendes Verhalten in jedem Stadium der primären Sozialisation möglich, ohne daß diese erhöhte Delinquenz notwendig zu kriminellen Karrieren führt. Bisher konnte es sogar geschehen, daß die Erziehungsberechtigten von dem Anlegen einer Kriminalakte über ihr strafunmündiges Kind nicht einmal unterrichtet wurden.

Es ist daher zu überlegen, ob und inwieweit Kinderdelinquenz überhaupt in polizeilichen Akten dokumentiert werden soll. Wenn man bedenkt, daß das Ziel des erweiterten Erwachsenenstrafrechts primär die Resozialisierung des Täters, mit anderen Worten seine Entkriminalisierung ist, ist es auf der anderen Seite kaum hinzunehmen, daß durch die Aufnahme von Kinderdelinquenz in Kriminalakten nicht Strafmündige bereits im Kindesalter als „kriminell“ etikettiert werden. Nichts anderes meint auch das Bundesverwaltungsgericht, wenn es die Speicherung in polizeilichen Akten grundsätzlich als Eingriff in das allgemeine Persönlichkeitsrecht – hier des Kindes – wertet.

Zu erwägen bleibt daher, ob Delinquenz von strafunmündigen Kindern nicht ausschließlich bei denjenigen staatlichen Stellen geführt werden muß, die einen subsidiären staatlichen Erziehungsauftrag haben, wie z. B. die Jugend- und Sozialämter. Inwieweit also die Speicherung von Kindern bei der Polizei erforderlich ist, richtet sich nach der rechtspolitischen Entscheidung, ob Kinderdelinquenz primär als Aufgabe präventivpolizeilicher Gefahrenabwehr definiert wird oder ob der Kinderdelinquenz vor allem durch Instanzen sozialer Kontrolle mit Erziehungsaufgaben begegnet werden kann.

Gespräche mit Vertretern des HLKA und HMdI haben zwar Verständnis für meine Position seitens der Kriminalpolizei erkennen lassen, dennoch wurde von ihnen dem Gesichtspunkt polizeilicher Gefahrenabwehr die Priorität eingeräumt. Immerhin hat sich Konsens wenigstens soweit erzielen lassen, als der Hessische Minister des Innern im Arbeitskreis II der Innenministerkonferenz der Länder beantragt, in die KpS eine Bestimmung einzufügen, die vorsieht, daß die Erziehungsberechtigten bei Kindern über die Anlage von KpS zu unterrichten sind, es sei denn, daß das öffentliche Interesse an der Geheimhaltung oder das Wohl des Kindes berührt wird. Obendrein soll die regelmäßige Prüfung für die Aussonderung von Kinderakten bei Bagatelldelikten auf ein Jahr, bei Jugendli-

chen auf zwei Jahre verkürzt werden. Auch die vom Hessischen Minister des Innern vorgeschlagene Änderung zu Ziffer 8.3.5 KpS (Aussonderungsfristen für Kinderdelinquenz und die Jugendstraftaten) ist erheblich gegenüber der ursprünglichen Fassung der AG Kripo verbessert worden. Danach dürfen KpS bei Kindern über drei Jahre, bei Jugendlichen über vier Jahre hinaus nur dann aufbewahrt werden, wenn

- „bei Kindern aufgrund der Anzahl oder der besonderen Sozialschädlichkeit der bisher vorgeworfenen Delikte sowie der dabei aufgewandten kriminellen Energie davon ausgegangen werden muß, daß sie weiterhin rechtswidrige Taten begehen werden oder daß die Unterlagen aus Gründen der Gefahrenabwehr (z. B. Vermißte) auch zukünftig erforderlich sind;
- bei Jugendlichen aufgrund der Anzahl und Art der bisher vorgeworfenen Delikte davon ausgegangen ist, daß sie weiterhin rechtswidrige Taten begehen werden und dabei die Unterlage zu Zwecken gemäß Nr. 2 oder zur Durchführung des Jugendstrafverfahrens (§ 43 JGG) erforderlich sind.“

Auch wenn also meinen Anregungen nicht in vollem Umfang gefolgt worden ist, sind doch diese Regelungen als ein erheblicher Fortschritt im Vergleich zur bisherigen Rechtslage anzusehen. Allerdings wird die Praxis der Aussonderung erweisen müssen, ob die mit KpS erklärte Bereitschaft der Polizei zu datenschutzgerechtem Handeln sich als realistisch erweist, oder ob die ins Auge gefaßte Aussonderung schließlich an dem befürchteten Verwaltungsaufwand scheitert bzw. bis zur endgültigen Regelung einer zentralen Erschließung der überregionalen Dateien im polizeilichen Informationssystem (Inpol) über den Zentralen Personenindex nur teilweise stattfindet.

Das hier angesprochene Problem wird besonders anschaulich am Falle einer jungen Frau, die sich mit der Beschwerde wegen unzulässiger Datenspeicherung durch die Polizei an mich gewandt hatte. Als ehrliche Finderin hatte die junge Frau einen größeren Geldbetrag, den sie auf der Straße gefunden hatte, beim nächsten Polizeirevier abgegeben. Der diensthabende Beamte notierte ihre Adresse und telefonierte dann kurz. Daraufhin bemerkte er gegenüber der jungen Frau, sie sei wohl auch der Polizei keine Unbekannte mehr und sei schon wegen Betruges in Erscheinung getreten. Auf ihre empörte Frage

deutete der Beamte an, daß er diese Information soeben telefonisch bekommen habe. Die Prüfung der Beschwerde ergab, daß die Beschwerdeführerin als Kind im Alter von 13 Jahren zusammen mit Schulfreundinnen versucht hatte, beim Ziehen einer Zigarettenpackung aus dem Automaten (nach Einwurf des Geldbetrages) mit Hilfe ihres Stielkammes eine weitere Packung (ohne Bezahlung) herauszumanövrieren. Dabei war sie als einzige erwischt worden, hatte aber später nie mehr etwas von der Sache gehört: insbesondere waren weder sie noch ihre Eltern darüber informiert worden, daß eine Kriminalakte über sie angelegt worden war. Der Vorfall lag inzwischen über acht Jahre zurück:

Es steht außer Diskussion, daß der diensthabende Beamte zu dieser Bemerkung nicht berechtigt war und damit gegen seine Dienstvorschriften verstoßen hat. Das Bedenkliche des Falles liegt darin, daß in einem solchen Bagatellfall – der eher in den Bereich der Jugendstreiche als in den der Kriminalität gehört – überhaupt eine Kriminalakte angelegt wurde, daß dies weder der Betroffenen selbst noch ihren Eltern bekannt war, und daß die Angelegenheit als „Betrugsfall“ über acht Jahre im Hessischen Polizeiinformationssystem (HEPOLIS) gespeichert blieb. Es ist kaum auszudenken, welchen Schaden die Betroffene gehabt hätte, wenn sie die Fundanzeige zufällig in Begleitung von guten Freunden, Verwandten oder ihres Chefs gemacht hätte. Dabei muß jedoch betont werden, daß der Polizeidienststelle, die seinerzeit die Akte anlegte und die Angaben in HEPOLIS einspeicherte, deswegen kein Vorwurf gemacht werden kann: Sie handelte im Rahmen der bisher geübten Praxis, die für solche Fälle eine zehnjährige Speicherung zuließ. Auch konnte ich mich davon überzeugen, daß aufgrund der Beschwerde der Betroffenen die Akte inzwischen vernichtet und die Speicherung gelöscht worden war. Dabei räumte der Vertreter des zuständigen Polizeipräsidiums ein, der einzelne Revierbeamte sei manchmal bei der Frage, ob eine Kriminalakte angelegt werden müsse oder nicht, überfordert: Oft sei der Automatenmißbrauch das erste Glied in einer Kette, die über Autoaufbrüche und Ladendiebstähle zu einem kriminellen Lebenslauf führe. Bei einem Erstdelikt könne man so etwas nie mit Sicherheit voraussehen.

Zwar sehen die neuen KpS bezüglich der Aufbewahrung von Kriminalakten und einer

Speicherung in Polizeiinformationssystemen vor: Bei Kindern ist nach drei Jahren, bei Jugendlichen nach vier Jahren zu prüfen, ob eine Aussonderung möglich ist. Ausgesonderte Unterlagen müssen vernichtet werden; bei Speicherung auf elektronischen Datenträgern sind die Daten physisch zu löschen. Diese Verbesserungen sind zu begrüßen. Aus der Sicht des Datenschutzes bleiben aber trotzdem Bedenken bestehen. Es mag sein, daß die kriminologischen Erfahrungen der letzten Jahres es nicht als vertretbar erscheinen lassen, über Kinder, die strafunmündig sind, überhaupt keine Kriminalakten anzulegen. Auch das Argument, daß die Einspeicherung in Informationssysteme wie HEPOLIS gegenüber dem klassischen Verfahren der Telex-Anfrage „an alle“ und einer entsprechenden Neuanlage von Kriminalakten bei zahlreichen Polizeidienststellen eine geringere Gefährdung des Persönlichkeitsrechts der Betroffenen bewirkt, hat etwas für sich: Beim HEPOLIS-Verfahren wird nur an einer Stelle eine Akte über den Betroffenen geführt, und jede Polizeidienststelle kann durch Anfrage bei HEPOLIS feststellen, wo dies der Fall ist. Jedoch ist das Anlegen von Kriminalakten über strafunmündige Kinder und deren Speicherung in HEPOLIS ein schwerwiegender Eingriff nicht nur in das Persönlichkeitsrecht der Kinder, sondern auch das Erziehungsrecht der Eltern. Insbesondere die Speicherung von Kindern in einem zentralen Informationssystem der Polizei birgt Risiken, die nicht in jedem Falle überschaubar und damit auszuschließen sind. Die Abgrenzung zwischen den Schutzinteressen der Allgemeinheit im Rahmen der Verbrechensbekämpfung und dem Persönlichkeitsschutz des Kindes muß der Gesetzgeber treffen. Ohne gesetzliche Grundlage darf es keine Speicherung strafunmündiger Kinder in Polizeicomputern geben. Dabei halte ich es für erforderlich, eine Benachrichtigung der Erziehungsberechtigten für den Fall vorzusehen, daß über ein Kind eine Kriminalakte angelegt wird oder eine Speicherung in einem Polizeiinformationssystem erfolgt. Nur so wird gewährleistet, daß die Einhaltung der in den KpS vorgesehenen Lösungsfristen auch kontrolliert werden kann. Schließlich kann auch nur mit Hilfe der Erziehungsberechtigten der von der Polizei angestrebte Präventionseffekt nachhaltig erreicht werden. Insbesondere halte ich es für notwendig, eine Schwelle festzulegen und so präzisieren, daß Bagatellfälle, wie der am Beispiel der jungen Frau geschilderte, nicht mehr zur Anlegung einer Kriminalakte führen.

Bezüglich der bei der Polizei bereits vorhandenen Akten über Kinder können die Richtlinien für kriminalpolizeiliche Sammlungen in ihrer jetzigen Fassung ein gewisses Maß an Abgrenzung zwischen Individualrecht des Betroffenen und Schutzinteressen der Allgemeinheit bringen.

Da behördeninterne „Richtlinien“ aber ohne „Drittwirkung“ sind, dem Betroffenen also keine Rechte gewähren, können die KpS nur für eine Übergangszeit als ausreichend betrachtet werden.

Darüber hinaus muß sehr wohl überlegt werden, ob die von der Polizei für Erwachsene angewendeten Fahndungsverfahren für Kinder ebenso in Frage kommen können. Bei Kindern besteht ein besonderes Interesse, eine unkontrollierbare Verteilung von Informationen zu verhindern.

Ich verkenne nicht die Schwierigkeiten, die mit der Verwirklichung meiner Vorschläge verbunden sind. Bei dem bisher bestehenden erfreulichen Erfahrungsaustausch und der guten Zusammenarbeit zwischen dem Hessischen Innenministerium, den Polizeibehörden und meiner Dienststelle habe ich jedoch keinen Zweifel, daß in gemeinsamer Bemühung entsprechende Vorschläge für den Gesetzgeber gemacht werden können. Auf lange Sicht gesehen, scheint mir dies der beste Weg, die Effektivität der polizeilichen Arbeit zu erhalten und trotzdem die Forderungen des Datenschutzes zu respektieren.

2.3.3 ¹ Zur Auskunftregelung bei Sicherheitsbehörden

Die Vorschrift des § 18 Abs. 2 HD SG (entspricht wörtlich § 13 Abs. 2 BDSG), die eine generelle Ausnahme der Sicherheitsbehörden vom Auskunftsanspruch des Bürgers enthält, wirkt sich in der Praxis negativ auf meine Arbeit aus. Die Folge der Ausnahme ist, daß die Bürger, denen zum Beispiel von der Polizei oder dem Verfassungsschutz eine Auskunft darüber verweigert worden ist, ob sie in den Dateien dieser Behörden gespeichert sind, sich gemäß § 27 HD SG an mich wenden; denn das Anrufungsrecht nach § 27 HD SG unterliegt keiner Einschränkung. Jedermann kann sich an den Hessischen Datenschutzbeauftragten wenden, um zu erfahren, ob er selbst Betroffener im Sinne des Datenschutzgesetzes ist; er braucht dafür nur geltend zu machen, er nehme dies an und glaube dadurch in seinen Rechten verletzt worden zu sein. Zwar habe ich gemäß § 28

HDSG die Möglichkeit, die entsprechende Auskunft – ob der Bürger X in den Dateien der Sicherheitsbehörden gespeichert ist – zu erhalten. Ich bin auch verpflichtet, einer Eingabe nach § 27 nachzugehen und von meinen Befugnissen nach § 28 Gebrauch zu machen. Daher habe ich zu prüfen, ob die Annahme des Betroffenen, er werde in seinen Rechten durch eine Datenverarbeitung bei den Sicherheitsbehörden verletzt, zutrifft oder nicht. Ich bin ferner verpflichtet, die Eingabe zu bescheiden. Hierbei muß ich allerdings das Auskunftsverweigerungsrecht, das den genannten Behörden gegenüber dem Betroffenen zusteht, berücksichtigen; und zwar auch dann, wenn zur Person des Betroffenen keine Daten gespeichert sind, sondern nur die Frage geklärt werden soll, ob dies der Fall ist. Es entspräche allerdings nicht dem Sinn und dem Zweck des Gesetzes, auf eine solche Eingabe nur zu antworten, daß dem Betroffenen kein Auskunftsrecht zustehe, und daß deswegen auch der Datenschutzbeauftragte ihm keine Hilfe leisten könne. Wenn dies so gewollt wäre, hätte in § 27 eine Ausnahme für die in § 17 Abs. 2 Nr. 1 und 2 genannten Behörden (Sicherheitsbehörden) gemacht werden müssen.

Aus dieser Rechtslage folgt für den Datenschutzbeauftragten die schwierige Frage, in welcher Weise er seiner Verpflichtung, den Fragesteller zwar zu bescheiden, gleichzeitig aber zu beachten, daß dem Betroffenen kein Auskunftsrecht gegenüber den Sicherheitsbehörden zusteht, nachkommen kann. Meine Nachricht an den Betroffenen hat etwa folgenden Inhalt:

Zunächst einen Hinweis auf die Ausnahme der Sicherheitsbehörden von der allgemeinen Verpflichtung der Behörden und sonstigen öffentlichen Stellen des Landes, „dem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen“, gemäß § 18 Abs. 2 HDSG. Dann eine Information über meine Befugnis, auch bei den Sicherheitsbehörden die Einhaltung der Datenschutzbestimmungen zu überprüfen, mit der Einschränkung allerdings, die hierbei gewonnenen Erkenntnisse im einzelnen nicht mitteilen zu dürfen. Schließlich die Erläuterung, daß ich als Ergebnis nur bekanntgeben dürfe, ob der Betroffene in seinen Rechten verletzt sei, oder ob diese seine Vermutung nicht zutreffe. Diese Erläuterung wird mit der Feststellung abgeschlossen, ob meine Prüfung Anhaltspunkte für eine Beeinträchtigung schutzwürdiger Belange des Betroffenen ergeben hat oder nicht.

Vielfach und in zunehmendem Maße fühlen sich Betroffene durch diese „nichtssagende Auskunft“ ungenügend unterstützt, um nicht zu sagen: nicht ernst genommen. Dabei richtet sich ihr Unmut nicht gegen die Behörde, von der sie keine Auskunft erhalten können (Sicherheitsbehörde), sondern gegen den Hessischen Datenschutzbeauftragten, weil dieser vermeintlich seiner Funktion als „Anwalt des Bürgers“ nicht genügend nachkomme.

Die generelle Ausnahme der Sicherheitsbehörden vom Auskunftsanspruch des Bürgers in Abs. 2 des § 18 HDSG – zusätzlich zu der speziellen Ausnahme unter den Voraussetzungen von § 18 Abs. 3 HDSG – ist überflüssig und sollte gestrichen werden. Die Kommentierungen zum – wortgleichen – § 13 Abs. 2 BDSG lassen darüber keinen Zweifel, daß aufgrund dieser Bestimmung die Auskunft verweigert werden kann, aber nicht verboten ist und daß es insoweit bei der vor Inkrafttreten der Datenschutzgesetze bestehenden Rechtslage verbleibt, daß nämlich die Auskunftserteilung im pflichtgemäßen Ermessen der zuständigen Behörden liegt. Diese Ermessensentscheidung wird von den Sicherheitsbehörden auch praktiziert: In mehreren Fällen, in denen ich von Betroffenen um Überprüfung gebeten wurde, „... ob ich noch in den Dateien der Polizei (des Verfassungsschutzes) gespeichert bin ...“ und darauf hingewiesen hatte, daß ich weder eine positive noch eine negative Aussage zur Speicherung selbst abgeben könne, haben mich Betroffene darauf hingewiesen, die Polizei (der Verfassungsschutz) habe ihnen bereits mitgeteilt, daß sie gelöscht bzw. nicht gespeichert seien; ihre Bitte an mich richte sich nur darauf, daß sich der Datenschutzbeauftragte über die Richtigkeit dieser Angaben vergewissern solle.

Zur weiteren Begründung meines Vorschlags auf Streichung von § 18 Abs. 2 HDSG muß ich darauf hinweisen, daß diese Vorschrift über die generelle Ausnahme der Sicherheitsbehörden von dem Auskunftsanspruch des Bürgers durch die Bestimmungen über die Datenlöschung, nämlich § 19 Abs. 3 S. 2 i. V. m. § 19 Abs. 2 S. 2 HDSG, umgangen werden kann: Da unstreitig dieser Löschungsanspruch nicht den Einschränkungen wie der Auskunftsanspruch im Hinblick auf die Sicherheitsbehörden unterliegt, wird von manchen Betroffenen aufgrund der genannten Bestimmungen bei der zuständigen Sicherheitsbehörde die Löschung der über sie gespeicherten Daten verlangt. Ergibt die daraufhin von der zuständigen Behörde anzustellende Überprü-

fung, daß die über den Betroffenen gespeicherten Daten zur rechtmäßigen Erfüllung der in der Zuständigkeit der Behörde liegenden Aufgaben nicht mehr erforderlich sind, so muß sie diese löschen. Dabei wird das pflichtgemäße Ermessen in der Regel eine Mitteilung über die Löschung erlauben. Das gleiche gilt, wenn die Behörde feststellt, daß keinerlei Daten über den Betroffenen gespeichert sind, also auch nicht gelöscht werden können. Es wäre vollkommen ausreichend, wenn die Ausnahme von der Auskunft bei den Sicherheitsbehörden nicht generell bestimmt würde, sondern nur im Einzelfall, wie dies § 18 Abs. 3 ohnehin bereits vorschreibt. Dies würde auf der einen Seite ermöglichen, daß dort, wo die Arbeit der Sicherheitsbehörden nicht tangiert ist, durch die Auskunftserteilung eine größere Transparenz ihrer Arbeit erreicht wird. Dies wiederum könnte bei der Mehrzahl der Auskunftersuchen, die völlig „harmlos“ sind, ein größeres Vertrauen der Bürger zu den Sicherheitsbehörden bewirken. Zum anderen ließe sich durch eine solche Lösung erreichen, daß die Arbeit des Hessischen Datenschutzbeauftragten auf diesem Gebiet wesentlich entlastet würde und er darüber hinaus nicht in Gefahr wäre, dem Bürger gegenüber unverdient in die Rolle des „Prügelknaben“ zu geraten.

2.3.4 Telefonische Auskunftersuchen der Polizei an Kraftfahrzeug-Zulassungsstellen und Einwohnermeldeämter

Immer mehr Kfz.-Zulassungsstellen und Einwohnermeldeämter sind dazu übergegangen, telefonischen Anrufern die Auskunft über personenbezogene Daten zu verweigern, wenn sich der Anrufer nicht zweifelsfrei identifizieren kann.

Da aber andererseits die Notwendigkeit bestand, den Amtshilfeersuchen insbesondere der Polizeibehörden bei telefonischen Anfragen in eiligen Fällen nachzukommen, wurden versuchsweise in Teilbereichen Code-Worte verwendet, die den Anrufer bei der betroffenen Behörde identifizieren sollten.

Das Hessische Landeskriminalamt hat nach ersten Erfahrungen mit dieser Verfahrensweise dem Hessischen Minister des Innern einen Bericht vorgelegt und darum gebeten, auf einen weiteren Einsatz der teilweise eingeführten Code-Worte zu verzichten. Als Grund wurde insbesondere die größere Behinderung der polizeilichen Ermittlungsarbeit angeführt und darauf hingewiesen, daß der gewollte Sicherungseffekt durch die weite Verbreitung der Code-Worte bei den einzelnen Polizei-

dienststellen des Landes bis hinunter zum diensthabenden Polizisten unterlaufen werde. Das Hessische Landeskriminalamt schlug dagegen vor, den telefonischen Rückruf durch die angerufene Stelle wieder einzuführen. Der Hessische Minister des Innern hat sich dieser Argumentation angeschlossen und um meine Stellungnahme gebeten.

Ich habe dem Hessischen Minister des Innern mitgeteilt, daß ich den telefonischen Rückruf für ein zweckmäßiges Mittel zur Berichtigungsprüfung halte und angeregt, das geschilderte Auskunftsverfahren durch Dienstanweisung bei den Einwohnermeldeämtern und Kfz.-Zulassungsstellen sicherzustellen. Darüber hinaus sollte der Kreis der autorisierten Stellen und deren dienstliche Telefonnummern bei den betroffenen Dienststellen bekannt gemacht werden.

2.3.5 Bundeszentralregister und kriminalpolizeiliche personenbezogene Sammlungen

Die bereits in meinem letzten Tätigkeitsbericht aufgeworfene Frage, inwieweit § 49 Bundeszentralregistergesetz (BZRG) der Speicherung und Verarbeitung bereits getilgter Verurteilungen und den ihnen zugrundeliegenden Taten in Dateien und Informationssammlungen der Polizei entgegensteht, hat im Berichtszeitraum weitgehende Klärung erfahren. Sowohl die Erörterung dieser Frage in der vom Innenausschuß eingesetzten Arbeitsgruppe Datenschutz und die parallel dazu verlaufenden intensiven Bemühungen der Innenministerkonferenz um Entwurf und Einführung von Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) (vgl. 2.3.1) haben zu einer Annäherung kontroverser Standpunkte geführt und Lösungsmöglichkeiten im Sinne eines effektiven Datenschutzes zugunsten des betroffenen Bürgers aufgezeigt.

Das Bundeszentralregister regelt unzweifelhaft nicht unmittelbar die Führung von Akten bei der Kriminalpolizei. Hieraus jedoch die Schlußfolgerung zu ziehen, daher habe das BZRG keine Auswirkung auf die Führung polizeilicher Dateien, ist in der Tat ein Fehlschluß. § 49 BZRG findet als Vorhaltungs- und Verwertungsverbot auch auf polizeiliche personenbezogene Sammlungen Anwendung. Hierbei fallen Tat und Beurteilung unter das Vorhaltungs- und Verwertungsverbot. Dabei ist die Tat im strafprozessualen Sinn (§ 264 StPO) zu definieren, umfaßt also den gesamten tatsächlichen Vorgang, der Gegenstand der Urteilsfindung war. Eine

Verwertung zum Nachteil liegt nach herrschender Meinung stets dann vor, wenn aus der Tat oder der Verurteilung ungünstige Folgerungen gezogen werden (Albrecht Götz, Das BZRG, Kommentar, 2. Aufl. 1977, Anm. 13 zu § 49 BZRG S. 129). Daraus folgt, daß z. B. weder bei der Strafzumessung (vgl. BGHSt 24, 378; BayObLG in: MDR 72, 443) noch bei der Verwertung als Indiz für die Begehung einer gleichartigen oder ähnlichen Tat auf eine Eintragung im Bundeszentralregister zurückgegriffen werden darf (vgl. auch BVerfGE 36, 174).

Nun hat der Bundesminister des Innern den Innenministern der Länder seine Stellungnahme, die von dem Bundesminister der Justiz geteilt wird, zum Verwertungsverbot des § 49 BZRG mitgeteilt, die er gegenüber dem Bundesbeauftragten für den Datenschutz abgegeben hat. Er führt dort unter anderem aus:

„Ich teile die Auffassung des Bundesministers der Justiz, daß nach Eintritt der Tilgungsreife die Verurteilung oder die ihr zugrunde liegende Tat bei polizeilichen Ermittlungen nicht als Indiz für die Begehung weiterer Straftaten herangezogen werden dürfen. Dies schließt eine Weitergabe dieser Erkenntnisse innerhalb der Polizei zur rechtmäßigen Aufgabenerfüllung allerdings nicht aus. Diese Übermittlung ist keine „Verwertung im Rechtsverkehr zum Nachteil des Betroffenen“, sondern Mittel zur objektiven Aufklärung des Sachverhalts. Es dürfen allerdings der Tilgungsreife unterliegende Erkenntnisse

dem Betroffenen nicht vorgehalten und

nicht als Überführungstatsache (Indiz) etwa in Schlußberichten, Anklageschriften usw. verwendet werden.“

Diese Auffassung widerspricht der Rechtsprechung des Bundesverfassungsgerichts sowie der oberen Bundesgerichte und den verfassungsrechtlich verankerten Grundsätzen des Datenschutzes. Darüber hinaus wird durch diese Auffassung die Grundintention des Gesetzgebers des BRZG konterkariert. So umfaßt nach ständiger Rechtsprechung (vgl. BVerfGE 36, 174; OVG Münster NJW 74, 1714) der Begriff des Rechtsverkehrs alle Bereiche des Rechtslebens, neben Straf- und Verfahrensrecht also z. B. auch das Privat-, Arbeits-, Sozial- und Verwaltungsrecht. Zutreffend führt der Hessische Verwaltungsgerichtshof im Urteil vom 3. Dezember 1973 –

Az: VI OE 28/71 – aus, zum Rechtsverkehr gehörten auch die Beziehungen zwischen Bürger und den Verwaltungsbehörden, was sich insbesondere aus den Ausnahmebestimmungen in § 49 Abs. 2 und § 50 BZRG entnehmen lasse.

Spätestens seit dem bekannten Urteil des Bundesverwaltungsgerichts zur vorbeugenden erkennungsdienstlichen Behandlung im 26. Band S. 159 ff. ist für jedermann deutlich, daß auch das Informationsverhalten der Polizei dem verfassungsrechtlichen Verhältniseitsgebot unterliegt. Mit anderen Worten, es gibt kein tatsächliches Informationsverhalten, daß außerhalb des „Rechtsverkehrs“ stattfindet. Vielmehr wird es durch ein komplexes Normenbündel im Verhältnis zum Bürger geregelt und kann nur in den Grenzen des Verhältnismäßigkeitsprinzips stattfinden. Nach alledem ist eine Verwertung der Tat und der Verurteilung im Rechtsverkehr zu Lasten des Betroffenen nach der Tilgungsreife im BZRG in polizeilichen Dateien – ebenso wie in anderen Dateien – unzulässig. Das Verwertungsverbot hat zudem konkrete datenschutzrechtliche Folgen: Gemäß § 19 Abs. 2 S. 2 HDSG sind diese Daten durch die Polizei zu sperren bzw., wenn der Betroffene es verlangt, zu löschen (§ 19 Abs. 3 HDSG, wenn die Tilgungsreife nach dem BZRG eingetreten ist).

Das Verwertungsverbot findet also seine komplementäre Konkretisierung in Datenschutzgesetzen des Bundes und der Länder für die Fälle, in denen Angaben über Tat und Verurteilung im BZRG selbst der Tilgungsreife unterliegen.

2.4 Datensicherung

2.4.1 Entwurf eines Maßnahmenkatalogs zur Datensicherung

Wer personenbezogene Daten verarbeitet, hat nach § 6 BDSG technische und organisatorische Maßnahmen zu treffen, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Für die automatisierte Verarbeitung personenbezogener Daten ist ein Katalog von zehn Kontrollen in der Anlage zu § 6 Abs. 1 S. 1 BDSG aufgestellt. Diese Vorschriften finden sich wortgleich in § 10 HDSG und der Anlage zu diesem Paragraphen wieder. Eine Besonderheit dieser Vorschriften ist, daß der Gesetzgeber in Anwendung des Prinzips der Verhältnismäßigkeit Maßnahmen nur dann für erforderlich hält, wenn ihr Aufwand in

einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Im Gegensatz zu einer im Regierungsentwurf eines BDSG vorgesehenen Verordnungsermächtigung für den Bundesminister des Innern, der Grundsätze über entsprechende (Sicherungs-) Maßnahmen aufstellen und auch bestimmte Maßnahmen vorschreiben sollte, sieht die jetzt gültige Regelung nur bestimmte zu erfüllende Funktionen vor und überläßt es im übrigen den datenverarbeitenden Stellen, geeignete Maßnahmen auszuwählen. Diese Regelung hat den Vorteil, daß sie Rücksicht auf die technische Entwicklung nimmt, die festgeschriebene Maßnahmen schnell überrollen könnte. Sie hat aber auch den Nachteil, daß durch die unscharfe Formulierung die Gefahr besteht, bei der Abwägung zwischen angestrebtem Schutzzweck und den entstehenden Kosten zugunsten der Wirtschaftlichkeit das Sicherungsniveau möglichst niedrig zu halten.

Im Interesse des Bürgers müssen jedoch „standards“ angestrebt werden, die eine weitgehend einheitliche Beurteilung ermöglichen. D. h. gleiche Tatbestände müssen gleiche Würdigung erfahren oder, an einem Beispiel gesagt, die Anforderungen, die der Hessische Datenschutzbeauftragte nach § 10 HDSG an eine hessische Behörde stellt, die Einwohnerdaten nach dem Melderecht verarbeitet, dürfen im wesentlichen nicht anders sein als die in einem anderen Bundesland. Zahlreiche Anfragen von speichernden Stellen nach dem „wie und was“ zu § 10 HDSG zeigen den Bedarf an einem Hilfsmittel zur Durchführung entsprechender Datensicherungsmaßnahmen.

Der bayerische Landesbeauftragte für den Datenschutz hat den Versuch unternommen, in enger Zusammenarbeit mit den Aufsichtsbehörden im Entwurf eines „Katalogs der Datensicherungsmaßnahmen gemäß § 6 BDSG bzw. Art. 15 Bayerisches Datenschutzgesetz“ ein funktionsfähiges Instrument zu entwickeln, das den dargestellten Problemen Rechnung trägt. Der Katalog geht dabei von der Erwägung aus, daß der Schutzzweck der Datenschutzgesetze darin besteht, zu verhindern, daß durch mißbräuchliche Verwendung personenbezogener Daten schutzwürdige Belange des Betroffenen verletzt werden. Als schutzwürdige Belange definiert er die Rechtsposition des Betroffenen, die er gegenüber Hoheitsträgern oder im Privatrechtsverkehr innehat, sowie alle Beziehungen, die er in seiner Umwelt aufgebaut hat, z. B. seine

gesellschaftliche Stellung, sein Ansehen oder seine wirtschaftlichen Verhältnisse. Die Wertung einer Verletzung dieser schutzwürdigen Belange versucht der Katalog in fünf Schutzstufen vorzunehmen, wobei die niedrigste Schutzstufe sog. frei zugängliche Daten enthält und die höchste Schutzstufe Daten, deren Mißbrauch Einfluß auf Gesundheit, Leben oder Freiheit des Betroffenen haben kann. Als Vorgehensweise werden zwei Schritte vorgeschlagen: Zunächst sollen die personenbezogenen Daten einer Datei auf ihre Schutzwürdigkeit hin überprüft und einer Schutzstufe zugeordnet werden, dann sind in Bewertung der entsprechenden Schutzstufe die erforderlichen Datensicherungsmaßnahmen auszuwählen.

Soweit der Maßnahmenkatalog den in § 6 BDSG aufgeführten Kontrollen detaillierte organisatorische und technische Maßnahmen zuordnet und diese in Schutzstufen gliedert, stellt er, so glaube ich, einen wesentlichen Fortschritt zu den bisher bekannten Checklisten dar.

Dagegen befürchte ich, daß der Lösungsansatz, als Kriterium für eine zu bestimmende Schutzwürdigkeit die (angenommene) Sensitivität von Einzeldaten zu nehmen, zu keinem brauchbaren Ergebnis führen wird. Es ist heute unbestritten, daß ein Datum immer nur in seinem Umfeld betrachtet werden kann; bei einem evtl. Kontextverlust kann sich z. B. der Gefährdungsgrad verändern. Und gerade hier liegt eine der Gefahren unkontrollierter Datenverarbeitung: Wir verarbeiten Informationen, Maschinen verarbeiten Daten³⁾. Wir hoffen dann, daß bei der Anwendung logischer Regeln die Maschine zum gleichen Ergebnis kommt wie wir, übersehen aber oft, daß das kennzeichnende Merkmal der automatisierten Datenverarbeitung eben der Kontextverlust ist.

Ein Beispiel: Der Bürger A hat bei der Firma B eine Ware gekauft. Nach Auslieferung stellt er fest, daß diese beschädigt ist und verweigert die Zahlung der Rechnung, bis einwandfreier Ersatz gestellt ist. Die Firma B mahnt den Kunden durch einen automatisierten Mahnbescheid und speichert im Kundenstammsatz das Datum „schlechter Zahler“. Durch den Kontextverlust, der dadurch eingetreten ist, daß die Umstände der Zahlungsverweigerung

³⁾ DIN Norm 40 300: „Zeichen oder kontinuierliche Funktionen, die zum Zweck der Verarbeitung Informationen aufgrund bekannter oder unterstellter Abmachungen darstellen“.

nicht gespeichert wurden, entsteht ein völlig falsches Bild der Zahlungsmoral des Kunden.

Weitere Beispiele für die Loslösung von Daten von ihrem eigentlichen Umfeld finden sich, wenn Daten gespeichert werden, ohne daß ihr Ursprung festgehalten wird. Wurden die Daten bei dem Betroffenen selbst oder an anderer Stelle erhoben? Zu welchem Zweck hat der Betroffene diese Angaben gemacht? Wie aktuell sind die Daten? Die Daten „Staatsangehörigkeit und Anschrift“ sind in dem Katalogentwurf in der Schutzstufe B (Belästigung) bzw. C. (evtl. Beeinträchtigung der gesellschaftlichen Stellung des Betroffenen) eingeordnet. Wenn jetzt aber – wie in der Vergangenheit geschehen – diese Daten bei einer Behörde abgerufen werden, weil aufgrund bestimmter politischer Vorgänge im Ausland Personengruppen einer evtl. Verfolgung unterliegen, müßten diese Daten nach dem Katalog in Schutzstufe F (Einfluß auf Gesundheit, Leben oder Freiheit des Betroffenen) eingestuft werden. Wie soll das aber geschehen, wenn bei einer vorangegangenen Einstufung diese Entwicklung nicht vorausgesehen werden konnte?

Das Dilemma ist auch von den Autoren des Maßnahmenkatalogs gesehen worden. An verschiedenen Stellen wird darauf hingewiesen, daß Datenfelder nicht einzeln klassifiziert werden dürfen; daß Dateien nur in ihrer Gesamtheit zu sehen sind; daß auf Verknüpfungsmöglichkeiten zu achten ist; daß der steigende Umfang der Daten über eine einzelne Person (Dossier) zu steigenden Schutzstufen führt usw. Diese Hinweise leisten aber keine Hilfestellung bei der Einschätzung der evtl. Sensitivität von Daten. Diese kann sich mit jeder geplanten Verarbeitung ändern. Versuche, Datengruppen bestimmten Sensitivitätsstufen zuzuordnen, sind in der Vergangenheit oft unternommen worden. 1972 hat Prof. Jon Bing von der Universität Oslo bei einem internationalen Symposium über „Data Banks and Society“ sein Modell einer Klassifizierung von Personalinformationen vorgestellt. Auch er hat Daten nach personenbeschreibenden Daten, Familienverhältnissen, häuslichen Verhältnissen, arbeitsrechtlicher Situation und anderen Kriterien zusammengestellt, um diese dann bestimmten öffentlichen Dateien zuzuordnen. Aus der so entstehenden Matrix sollte dann eine evtl. Sensitivität abgeleitet werden. Auch dieses Modell hat aufgrund der eingangs geschilderten Mängel keine Bedeutung erlangt.

Ein Patentrezept zur Lösung dieses Konflikts gibt es nicht. Möglicherweise fände sich ein Lösungsansatz, wenn die Problemanalyse anhand der Aufteilung des klassischen Verwaltungsaufbaus vorgenommen würde. D. h. Daten im Umfeld der Sicherheitsbehörden sind ohne weitere Untersuchungen ihrer Einzelsensitivität höher zu schützen als beispielsweise Adreßdaten eines Büros für Kongreßwesen in einer Großstadt; wer Querschnittsaufgaben in einem Großrechenzentrum der Verwaltung wahrnimmt, hat einen höheren Sicherheitsstandard zu erfüllen als derjenige, der in der Schule auf einer DV-Anlage, die vorwiegend Experimentierzwecken dient, auch nebenher zu Zwecken des Verwaltungsvollzugs Schüleradreßdaten speichert.

Um es noch einmal zu verdeutlichen: Die zwingende Notwendigkeit im Interesse des Bürgers, für den schließlich und endlich die Datenschutzgesetze geschaffen wurden, „standards“ zu finden, ist unbestritten. Das Problem liegt im Erkennen einwandfreier Bewertungskriterien.

Die Datenschutzbeauftragten des Bundes und der Länder haben bei ihrem gemeinsamen Treffen in München am 7./8. November 1979 den Entwurf des von dem Bayerischen Landesbeauftragten für den Datenschutz vorgelegten Maßnahmenkatalogs beraten und die Verabredung getroffen, Erfahrungen im praktischen Einsatz des Katalogs zu sammeln. Die in meiner Dienststelle anfallenden Erkenntnisse werden dann in einen Änderungsvorschlag einfließen.

2.4.2 Lösungsanspruch und Sicherungsdateien

Im Zusammenhang mit dem Begriff „löschen (Löschung)“ im Sinne des § 2 Abs. 2 Ziff. 5 HDSG ist es notwendig, sich mit dem Problem der Sicherungsdateien zu befassen.

2.4.2.1 Lösungsanspruch

Der Betroffene hat unter den in § 19 Abs. 3 HDSG genannten Bedingungen einen Anspruch auf Löschung seiner Daten. Der Begriff des „Löschens“ ist in § 2 Abs. 2 Ziff. 5 HDSG definiert⁴⁾.

⁴⁾ § 2 Abs. 2 Ziff. 5 HDSG (2) Im Sinne dieses Gesetzes ist 5. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren.

§ 19 Abs. 3 HDSG (3) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war oder wenn es in den Fällen des Abs. 2 S. 2 der Betroffene verlangt.

Dieses Gebot verpflichtet die speichernde Stelle Maßnahmen zu treffen, die eine künftige Informationsgewinnung aus gespeicherten und jetzt zu „löschenden“ Daten unmöglich macht. Mit anderen Worten, die Kenntnisnahme des Informationsgehaltes eines Datums durch den Einsatz von DV muß der speichernden Stelle unmöglich sein. Es genügt deshalb nicht, daß die speichernde Stelle durch Nutzungsverbote oder Zugangsbeschränkungen die Daten der Kenntnisnahme durch ihre Mitarbeiter entzieht. Eine Löschung liegt ebenfalls dann nicht vor, wenn die Daten im Zuge der physischen Beseitigung an anderer Stelle oder auf einem anderen Datenträger ohne Informationsverlust erneut gespeichert werden⁵⁾. Die Art der Informationsdarstellung spielt hierbei keine Rolle. Das bedeutet aber auch, daß nicht nur die Daten im jeweiligen aktuellen Datenbestand, sondern auch in allen angelegten Kopien zu löschen sind. Dies trifft die nach dem Generationsprinzip gesicherten Dateien ebenso wie die Systemaufzeichnung (Log-Dateien).

Aber genau an dieser Stelle zeichnet sich ein Zielkonflikt zwischen dem Erfordernis des Löschens und der Pflicht der speichernden Stelle ab, nach § 10 sowie der Anlage zu § 10 Abs. 1 S. 1 HDSG „technische und organisatorische Maßnahmen“ (zur Datensicherung) zu ergreifen.

2.4.2.2 Warum Sicherungsdaten?

Auch in der Datenverarbeitung ist es nicht zu vermeiden, daß durch Bedienungsfehler oder Versagen von technischen Einrichtungen Verarbeitungsläufe fehlerhaft durchgeführt werden. Tritt dieser Fall ein, muß der Lauf wiederholt werden. So einfach dies klingt, sind hierbei je nach Art der gewählten Technik erhebliche Probleme zu überwinden.

Bei der herkömmlichen Stapelverarbeitung treten die geringsten Probleme auf. Hier wird ein sequentiell aufgebauter Datenbestand „Alt“ mit einem ebenso sortierten Bestand „Änderungen“ verglichen und abgearbeitet. Als Ergebnis entsteht ein Datenbestand „Neu“. Tritt ein Verarbeitungsfehler auf, wird die Verarbeitung wiederholt, d. h. die Datenbestände „Alt“ und „Änderungen“ werden auf den den Anfang zurückgesetzt, das falsche Ergebnis „Neu“ gelöscht oder vernichtet und ein neuer Lauf gestartet. Unterstellt man aber, daß bei dem Verarbeitungslauf eine physische

Zerstörung eines oder mehrerer Datenträger eingetreten ist, z. B. durch mechanische Ursachen, so muß auf eine vorher gefertigte „Sicherungskopie“ zurückgegriffen werden, die den zu verarbeitenden Datenbestand in seinem ursprünglichen Zustand enthält. Üblicherweise werden drei solcher Kopien hergestellt, die nach dem Generationsprinzip aufbewahrt werden und auch als „Großvater-, Vater-, Sohn-“ Bänder bekannt sind. Das geschilderte Vorgehen gilt auch, wenn mit Direktzugriffsdateien gearbeitet wird. In diesem Fall wird der zu verändernde Datensatz in direktem Zugriff gefunden und auch direkt in der Datei geändert. Er ist also nach dem Änderungslauf nicht mehr in der ursprünglichen Form vorhanden. Die Wiederholung einer mißglückten Verarbeitung ist also nur möglich unter Verwendung einer Sicherungskopie. Tritt der Fehler am Ende mehrerer aufeinanderfolgender Änderungsläufe auf, und wurde nicht vor jeder Änderung ein Sicherungsbestand angelegt, müssen alle diese Läufe mit der vorhandenen Sicherungskopie wiederholt werden.

Wesentlich komplizierter wird der Fall, wenn – wie heute in weiten Bereichen üblich (Finanzwesen, Einwohnerwesen, Kfz.-Zulassung) – im sog. Online-Betrieb gearbeitet wird. D. h. alle Dateien stehen dem Anwender in direktem Zugriff zur Verfügung, Änderungen erfolgen über eine Datenstation in beliebiger Folge direkt in die Bestandsdatei. Selbst wenn diese vorher gesichert, also kopiert worden ist, so wären in diesem Fall aber keine Aufzeichnungen der vor oder während des Auftretens eines Fehlers durchgeführten Transaktionen vorhanden. Eine Wiederholung (restart) wäre damit unmöglich.

2.4.2.3 Log-Dateien

Dies ist ein Grund, warum in DV-Anlagen eingesetzte Betriebssysteme – das sind Programme der DV-Hersteller, die das Zusammenwirken aller Komponenten einer DV-Anlage steuern – die Systemaktivitäten aufzeichnen. Je nach der Art des eingesetzten Verfahrens – dieses ist u. a. wiederum abhängig von der Kapazität der vorhandenen DV-Anlage – werden auf einer ständig im Zugriff stehenden „Log-Datei“ die unterschiedlichsten Systemnachrichten gespeichert. Dies können z. B. sein: Datum und Uhrzeit der Transaktion, Urheber (Adressat) der Transaktion, an der Transaktion beteiligte Komponenten der DV-Anlage, Inhalt des Datensatzes vor und nach der Verarbeitung usw.

⁵⁾ Siehe auch Dammann in Simitis/Dammann/Mallmann/Reh, BDSG § 2 Rdnr. 134 ff.

Diese Log-Datei dient, wie erwähnt, primär der Datensicherung, d. h. sie ermöglicht die einwandfreie Wiederholung fehlerhafter Verarbeitungsläufe. Darüber hinaus bietet sich aber dem Anwender die Möglichkeit, bestimmte Leistungsdaten seines DV-Systems auszuwerten. Er kann statistische Auswertungen über die Belastung der Anlage, der externen Komponenten wie Terminals, Drucker oder auch Übertragungsleitungen, über die Verweildauer bestimmter Arbeiten (Jobs) in der Anlage und vor allem auch Abrechnungsdaten für externe Benutzer gewinnen.

Die geübte Verfahrensweise garantiert also die Datensicherung im kommerziellen Sinne. Aber sie erfüllt auch wesentliche Forderungen der nach § 10 bzw. der Anlage zu § 10 Abs. 1 S. 1 HDSG zu treffenden Maßnahmen. Beispielsweise kann festgestellt werden, wer oder welche Stelle Daten in ein DV-System eingegeben hat (Speicherkontrolle), eine Datenstation benutzt hat (Benutzerkontrolle) und damit welche Transaktion ausgelöst hat (Zugriffskontrolle) um nur einige Beispiele zu nennen. Damit stellt sich aber auch nicht mehr die Frage nach der Rechtmäßigkeit und Zweckmäßigkeit von Überwachungs- bzw. Sicherungsdateien (Log).

2.4.2.4 Der Konflikt

Der eingangs erwähnte Konflikt wird aber deutlich, wenn man die Anforderungen des „Löschens“ und der zu ergreifenden Datensicherungsmaßnahmen vergleicht. Denn, um es nochmals zu verdeutlichen, beim physischen Vorgang des Löschens wird der gelöschte Datensatz primär nur auf der Originaldatei gelöscht, er ist aber weiterhin in den Sicherungskopien enthalten und wird im Rahmen der Protokollierung der Systemaktivitäten **erneut** gespeichert, steht also jederzeit wieder zur Auswertung zur Verfügung.

2.4.2.5 Lösungsvorschlag

Einen Ausweg aus diesem Dilemma bietet nur die Lösung, daß die Löschung im – unter Beachtung der Sicherungsanforderungen – größtmöglichen Umfang und frühestmöglichen Zeitpunkt vorzunehmen ist.⁶⁾ Was bedeutet das?

1. Zu löschende, aber zu Sicherungszwecken noch aufbewahrte Daten dürfen ausschließlich im Sicherheitsfall und nur zur

Rekonstruktion der zerstörten Dateiinhalte und nur durch das beauftragte Personal eingesetzt werden.

2. Der Löschungspflicht ist unverzüglich, d. h. ohne schuldhaftes Zögern nachzukommen, wenn die gespeicherten Daten nicht mehr zu Sicherungszwecken benötigt werden. An die Bemessung der Frist ist ein strenger Maßstab anzulegen.
3. Bei der Aufbewahrung der Sicherungsdatei sind die erforderlichen technischen und organisatorischen Maßnahmen unter Beachtung des § 10 i. V. m. der Anlage zu § 10 Abs. 1 S. 1 HDSG zu treffen.

In den „vorläufigen Verwaltungsvorschriften“ zum Bundesdatenschutzgesetz, Abschnitt A Ziff. 5.5 hat der Ordnungsgeber einen ersten Ansatz gemacht, Teilbereiche dieses Problems in den Griff zu bekommen, wenn er ausführt: „Das Gesetz fordert nicht ein physisches Vernichten der Daten. Deshalb können z. B. einzelne Daten auf Sicherungsbändern auch dadurch gelöscht werden, daß durch geeignete organisatorische Maßnahmen sichergestellt ist, daß sie nicht mittels Datenverarbeitung zur Kenntnis genommen werden“.

Ich rege an, daß im Sinne einer einheitlichen Behandlung der Datensicherungsbestände die Landesregierung von der ihr in § 10 Abs. 4 HDSG eingeräumten Verordnungsermächtigung Gebrauch macht und (zumindestens für den Bereich der automatisierten Datenverarbeitung) entsprechende Vorschriften erläßt.

2.4.3 Vernichtung von Datenträgern

Wenn Maßnahmen erörtert werden, die dazu dienen sollen, die in § 1 HDSG definierten Ziele des Gesetzes unter Beachtung der in § 10 und der Anlage zu § 10 Abs. 1 S. 1 HDSG enthaltenen Vorschriften zu erreichen, stellt sich immer wieder das Problem der Vernichtung von Datenträgern.

2.4.3.1 Datenträger

Unter dem Begriff „Datenträger“ werden meist die speziellen Speichermedien der DV wie Magnetbänder, Magnetplatten, Lochstreifen, Lochkarten oder evtl. noch Druckprotokolle verstanden. Diese Eingrenzung ist jedoch zu eng. Einmal versteht das HDSG unter Datenverarbeitung auch bestimmte Arten der manuellen Verarbeitung von Daten, z. B. mittels Karteien, zum anderen faßt die DIN-Norm 44 300 den Begriff wesentlich weiter, wenn dort Datenträger als „...“

⁶⁾ Siehe auch Dammann in Simitis/Dammann/Mallmann/Reh, BDSG § 2 Rdnr. 135 ff.

jedes Mittel, auf dem Daten aufbewahrt werden können ...“ definiert wird. Damit dehnt sich der Kreis der zu beachtenden Datenträger über Band, Platte, Lochkarte aus und erfaßt auch Eingabebelege (Erfassungsbelege, Signierbelege), Magnetkarten, Karteikarten, Druckausgaben jeglicher Art – dazu gehört auch das Material aus Fehlläufen, also verdruckte Bescheide, Begleitlisten usw. –, Einwegkohlepapier und anderes.

Das bedeutet aber auch, daß Datenträger nicht nur im engsten Umfeld der Datenverarbeitung, also im Rechenzentrum zu finden sind, sondern in allen Bereichen der Verwaltung.

2.4.3.2 Zu beachtende Maßnahmen

Zuerst sei nochmals klargestellt: Die Vernichtung von Datenträgern erfüllt das Gebot des „Löschens“ und ist somit eine Phase der Datenverarbeitung. Dies wiederum bedeutet, daß auch beim Vernichten von Datenträgern die Vorschriften des HDSG insbesondere § 10 und die Anlage zu § 10 Abs. 1 S. 1 zu beachten sind. Dabei sollten folgende Grundsätze Anwendung finden:

1. Magnetbänder bzw. Magnetplatten

Auf magnetisierbaren Datenträgern gespeicherte Daten sind durch Überschreiben mit einem anderen Inhalt zu versehen oder mittels einem automatischen Bandreinigungsbzw. -löschgerät zu löschen. Herkömmliche Elektromagnete sind hierzu keinesfalls geeignet. Soll der Datenträger als solcher vernichtet werden, sind Bänder ggf. in geeigneten Anlagen zu verbrennen und Platten vor dem Verschrotten mechanisch unbrauchbar zu machen.

2. Mikrofilm und Mikrofiche

Mikroverfilmte Daten sind in einem derartigen Maßstab verkleinert (48 : 1 und kleiner), daß ein mechanisches Zerkleinern in einem herkömmlichen Papierreißwolf nicht ausreicht. Der entstehende Abfall enthält aufgrund seiner Schnittbreite von mindestens 4 bis 5 mm noch komplette Datensätze. Eine ordnungsgemäße Vernichtung ist nur bei Einsatz eines speziellen Mikrofilmvernichters, der die Filme zu pulverfeinem Staub zerkleinert, oder beim Verbrennen der Filme sichergestellt.

3. Papier

Datenträger auf Papierbasis wie Lochkarten, Lochstreifen, Ablochbelege, Erfas-

sungsbelege, Magnetkarten, Druckausgaben oder Einwegkohlepapier werden normalerweise einer Wiederaufbereitung im „recycling“ zugeführt. Dabei ist allerdings zu beachten, daß stark farbhaltige Papiere oder auch Kohlepapiere und selbstdurchschreibendes Papier für eine Wiederverwendung ausscheiden. Sie müssen in jedem Fall verbrannt oder mechanisch in einem Reißwolf so zerkleinert werden, daß der Abfall keine rekonstruierbaren Daten mehr enthält. Zur Wiederaufbereitung bestimmte Papiere, die besonders sensitive Daten enthalten, sind ggf. ebenfalls vor der Ablieferung an einen Verwertungsbetrieb durch einen Reißwolf vorzubehandeln. Die Aufbewahrung bis zur Vernichtung hat in geschlossenen Räumen oder entsprechenden Behältern zu erfolgen.

2.4.3.3 Auftragnehmer

Ist die Verarbeitung von Daten in einer vom Gesetz definierten Phase – also auch das Löschen bzw. Vernichten – durch einen Auftragnehmer vorgesehen, so ist dieser unter Beachtung der Vorschriften des § 4 HDSG auszuwählen. Besondere Beachtung ist dabei folgenden Punkten zu widmen:

1. Sorgfältige Auswahl eines zuverlässigen Unternehmens.
2. Vertragliche Festlegung der Pflichten:
 - 2.1 Unterwerfungserklärung unter das HDSG.
 - 2.2 Art des Vernichtungsverfahrens (Einstampfen, mechanisches Zerreißen, Verbrennen usw.).
 - 2.3 Art und zeitliche Begrenzung der Zwischenlagerung bis zur Vernichtung.
 - 2.4 Kontrollrechte der auftraggebenden Stelle.
 - 2.5 Haftungsfragen.
3. Transportmittel (gedeckter LKW, verschließbare Behälter) festlegen.
4. Transportweg abfahren und überprüfen.
5. Stichproben vornehmen.

2.4.4 DV-Entsorgungsspannen

Wie wichtig es ist, die dargestellten Probleme in den Griff zu bekommen, sei an folgenden „Pannen“ dargestellt, die mir im Berichtszeitraum bekanntgeworden sind.

2.4.4.1 Krankenkassen

Bei den Krankenkassen zugelassene Ärzte übertragen im Regelfall die Abrechnung ihrer Honorarforderungen mit den Krankenkassen an die Kassenärztlichen Vereinigungen. Die Honorarabrechnung des Arztes enthält die Personaldaten des Patienten, Angaben über den Arbeitgeber und bei Familienversicherten – das sind Familienmitglieder, die keine eigene Versicherung haben – auch die Daten des eigentlichen Versicherungsnehmers. Zur Begründung seiner Honorarforderung stellt der Arzt auf dem Beleg eine ausführliche Diagnose zu Beginn und am Ende der Behandlung, außerdem werden die einzelnen Behandlungsschritte offengelegt. Alles in allem, eine Sammlung höchst sensitiver Daten des Betroffenen. Die Kassenärztliche Vereinigung stellt diese Einzelbelege je Arzt nach den verschiedenen Krankenkassen zusammen und reicht sie dort zur Abrechnung ein.

Im Sommer dieses Jahres tauchte eine größere Anzahl solcher Belege bei der Redaktion einer großen Zeitschrift auf, die sich sofort mit mir in Verbindung setzte. Was war geschehen? Sofort eingeleitete Recherchen meiner Dienststellen ergaben folgenden Sachverhalt: Nach Auswertung der durch die Kassenärztliche Vereinigung eingereichten Unterlagen wurden diese von der Krankenkasse noch etwa 1 bis 2 Jahre aufbewahrt und dann einer Vertragsfirma zur Vernichtung übergeben. Der Transport der Belege von der Krankenkasse nach Frankfurt am Main – dort war der Unternehmenssitz des beauftragten Altpapierhändlers – erfolgte in verschürten Kartons, die auf einem gedeckten LKW von der Firma abgeholt wurden. Die Krankenkasse war im Besitz einer „Verpflichtungserklärung“ des Unternehmers, die aber in keiner Weise den Anforderungen des § 4 HDSG entsprach. Sichtproben oder Kontrollen bei dem Unternehmen selbst waren nicht erfolgt.

Das Firmengelände war leicht zugänglich, zu vernichtende Datenträger in einer zum Firmenhof hin offenen Halle gelagert. Die Art des Unternehmens bedingte es, daß als Arbeitskräfte lediglich nicht ausgebildetes Personal zum Einsatz kam, welches darüber hinaus teilweise nur stundenweise beschäftigt wurde. Der Unternehmer selbst bezeichnete sein Personal als nicht sehr zuverlässig. Eine Verpflichtung der dort Beschäftigten nach § 9 HDSG war nicht erfolgt. Das Unternehmen hatte keine Anordnung getroffen, wie lange und unter welchen Bedingungen zur Vernichtung angelieferte Datenträger gelagert werden

durften. Material mit sensitiven Daten war nicht getrennt von normalem Altpapier.

Eine Funktionsprüfung der von der Firma eingesetzten Papierzerreißmaschine, eines sog. „Shredders“ ergab, daß das Endprodukt eine Größe bis zum Format DIN A 6 aufwies; damit waren die Daten noch leicht lesbar und das Löschgebot des HDSG folglich nicht erfüllt.

Auf meine Anregung hin hat die Krankenkasse die Ablieferung von Datenträgern an dieses Unternehmen sofort gestoppt und das sensitive Material selbst eingelagert. Die Geschäftsleitung hat die Anschaffung eines eigenen Papierreißwolfs beschlossen. ADV-Abfälle werden künftig nur noch als Papierwolle mit einer Schnittbreite unter 4 mm abgeliefert. Darüber hinaus hat der Landesverband dieser Krankenkasse seine Mitglieder durch Fernschreiben auf den Fall hingewiesen und eine Überprüfung aller Auftragsverhältnisse im Rahmen der Vernichtung von Datenträgern gefordert.

Der Hessische Sozialminister hat diesen Vorfall zum Anlaß genommen, die seiner Aufsicht unterliegenden Verbände der Krankenkassen, die Landwirtschaftliche Krankenkasse Darmstadt, die Landesversicherungsanstalt Hessen, die landesunmittelbaren Unfallversicherungsträger sowie die Kassenärztliche und Zahnärztliche Vereinigung Hessen in einem Erlaß „Vernichtung von Akten und sonstigen Unterlagen im Bereich der Sozialversicherung“ auf die Einhaltung der Vorschriften des HDSG hinzuweisen.

2.4.4.2 Ordnungsamt

Einer hessischen Tageszeitung wurde von einem aufmerksamen Bürger ein Plastiksack mit Papierabfällen aller Art, darunter solche mit personenbezogenen Daten von Einwohnern, überbracht. Eine Kontrolle durch meine Dienststelle ergab, daß es sich offensichtlich um Büroabfälle des Ordnungsamtes – genauer gesagt, der Einwohnermeldestelle, der Paßstelle und der Abteilung Ausländerwesen – handelte. Neben offensichtlichem Müll enthielt der Plastiksack verschriebene Formulare mit personenbezogenen Daten, Mitteilungen anderer Behörden – sog. Rückmeldungen – oder auch standesamtliche Mitteilungen über Geburten, Heirat und Tod von Einwohnern.

Der Bürger, dem der Plastiksack neben einer gefüllten Abfalltonne am Hauseingang des Ordnungsamtes aufgefallen war, hatte mit Recht in dem sorglosen Umgang mit diesem

Material einen Verstoß gegen geltendes Datenschutzrecht gesehen. Meine Untersuchungen haben ergeben, daß eine Putzfrau in offensichtlicher Unkenntnis bestehender Anweisungen diese Abfälle aus Papierkörben des Amtes gesammelt und neben die Mülltonne gestellt hatte. Es stellte sich aber auch heraus, daß die Mitarbeiter des Amtes nur unzureichend über die Behandlung von Datenträgern mit personenbezogenen Daten unterrichtet waren. Die Amtsleitung hat auf meinen Hinweis sofort eine schriftliche Belehrung der Mitarbeiter durchgeführt, den Verschluß der Abfalltonnen angeordnet und sichergestellt, daß alle Datenträger mit personenbezogenen Daten durch einen Papierreißwolf vernichtet werden. Der Oberbürgermeister der betroffenen Stadt hat den Vorfall zum Anlaß genommen, eine Überprüfung aller städtischen Ämter durchführen zu lassen, um ähnliche Pannen künftig auszuschließen.

2.4.4.3 Sozialamt

Einer Bürgerin, die bei dem Sozialamt derselben Stadt einen Antrag stellen wollte, wurde hilfsbereit Konzeptpapier übergeben, damit sie sich einige Notizen machen konnte. Sehr erstaunt war sie allerdings, als sie zu Hause feststellte, daß sich das Konzeptpapier auf der bedruckten Vorderseite als eine Durchschrift eines computergedruckten Ablehnungsbescheides in einer anderen Sozialhilfesache herausstellte. Keine Frage, daß der Bescheid alle relevanten personenbezogenen Daten des Antragstellers wie Namen, Anschrift, Einkommen, Höhe der zu zahlenden Miete und anderes enthielt.

Meine Überprüfung ergab, daß aus falsch verstandener Sparsamkeit nicht benötigte Durchschriften aus den Genehmigungsverfahren als Notizpapier Verwendung fanden und somit diese Daten unbefugten Dritten zugänglich wurden. Durch Anordnung des zuständigen Dezernenten ist sichergestellt, daß sich dieser Fall künftig nicht wiederholt.

2.4.5 Datenschutz und dezentralisierte Datenverarbeitung

Der Wunsch, Verwaltungsaufgaben unter Einsatz der ADV möglichst rationell zu erledigen, war bisher meist von dem Zwang zur Zentralisierung begleitet. Die Entwicklung des Hessischen DV-Verbundes hat dies bestätigt. Immer umfangreichere und kompliziertere Verfahren wurden erarbeitet und in den Rechenzentren des Verbundes zentral für die

Anwender bereit gehalten. Hier zeichnet sich eine entscheidende Wende ab.

2.4.5.1 Technische Entwicklung

Wie ich bereits einleitend ausgeführt habe, hat die technische Entwicklung der letzten Jahre zu immer kleineren und zugleich leistungsfähigeren Komponenten der Datenverarbeitung geführt, bei denen das Preis/Leistungsverhältnis ständig günstiger wird. Als Folge davon ist zu beobachten, daß in zunehmendem Maße Computerleistung an die Arbeitsplätze zurückdelegiert wird. Beispielhaft hierfür sind umfangreiche Konzeptionen der Datenfernverarbeitung, wie z. B. im Finanzwesen, Einwohnerwesen und Kfz.-Zulassungswesen, wo der jeweilige Sachbearbeiter über ein Terminal (Bildschirm) direkten Zugriff zum Rechner hat, oder die Diskussion über den Einsatz verteilter Datenverarbeitung („distributed processing“), d. h. dezentrale Rechenanlagen vor Ort übernehmen einen großen Teil der ADV-Routine-Arbeit und bedienen sich lediglich in besonderen Fällen der größeren Speicher- und Rechenkapazität eines Großrechenzentrums, mit dem sie in einem Verbundnetz zusammengeschaltet sind.

2.4.5.2 Stapel-Verarbeitung

Den Datenschutz stellt diese Entwicklung allerdings vor neue, große Probleme. Bisher war es so, daß die einem DV-Verfahren angeschlossene (speichernde) Stelle einen schriftlichen Arbeitsauftrag an das Rechenzentrum erteilte und die evtl. benötigten Verarbeitungsdaten (Neuzugänge, Abgänge, Änderungen) auf Datenträgern, wie z. B. ADV-Belegen, Lochkarten oder Bändern an das Rechenzentrum gab. Die für die Arbeitsvorbereitung im Rechenzentrum zuständige Stelle prüfte die Zugriffsberechtigung des Auftraggebers, stellte die benötigten Dateien auf ihren Datenträgern bereit und terminierte den Verarbeitungslauf. Das Ergebnis wurde dann auf Richtigkeit und Vollständigkeit geprüft und dem Auftraggeber zugestellt.

Die Probleme des Datenschutzes, wie sie insbesondere bei der Speicherkontrolle, Eingabekontrolle, Auftragskontrolle oder Transportkontrolle auftraten, beschränkten sich im wesentlichen auf das Rechenzentrum und das unmittelbar beteiligte Personal. Im Regelfall waren sie durch bauliche und organisatorische Maßnahmen zu lösen.

2.4.5.3 Datenfernverarbeitung

Ganz anders jedoch stellt sich die Problematik bei DV-Anlagen, auf die im Wege der Datenfernverarbeitung zugegriffen wird. Sinn und Zweck der Verlagerung von Computer-Leistungen an den Arbeitsplatz sind nur dann erfüllt, wenn es gelingt, einer großen Anzahl von Stellen (Personen) gleichzeitig unter Anwendung einheitlicher Verfahren den Zugriff auf große Datenbestände zu ermöglichen, ohne daß dabei Belange des Datenschutzes verletzt werden. Hierbei treten jedoch größere Probleme im Bereich der Benutzerkontrolle, Zugriffskontrolle, Übermittlungskontrolle und Transportkontrolle auf.

Organisatorische und bautechnische Abschottung vor Ort vorausgesetzt, konzentrieren sich evtl. Schwachstellen auf das Übertragungsnetz und die Zugriffssicherung im Rechenzentrum. Niemand wird ernsthaft bezweifeln, daß es Experten möglich ist, mit dem entsprechenden Aufwand in jedes DV-System einzudringen. Bisher konnten von Menschen entwickelte Sicherungsmaßnahmen stets durch menschliche Intelligenz überwunden werden. Dazu gehört aber außer einer fundierten Kenntnis der Materie auch Zeit. Ziel aller zu treffenden Maßnahmen kann es also nur sein, mit angemessenen Mitteln einen möglichst hohen Schutzwall zu errichten. Hierzu gehören insbesondere:

1. Organisatorische und technische Maßnahmen bei den Verfahrensanwendern (speichernde Stellen) wie z. B. abschließbare Räume, verschließbare Terminals, organisatorische Festlegung der „Befugnisse“ der Mitarbeiter, sorgfältige Aufbewahrung von Eingabebelegen, Druckausgaben oder mikroverfilmten Daten.
2. Vorrangiger Einsatz von Standleitungen zur Datenübertragung. Wo dies aus Kostengründen nicht möglich erscheint, darf das Anwählen des jeweiligen Teilnehmers nur vom Rechenzentrum aus und möglichst automatisch erfolgen.
3. Einwandfreie und sichere Identifikation der beteiligten Datenstationen, möglichst über eingebaute elektronische Komponenten. Erst danach darf der Abruf oder das Senden von Daten erfolgen.
4. Einsatz von häufig wechselnden, dezentral verwalteten Kennungen auf Benutzerebene („user-id“), denen ein entsprechend tief gestaffeltes Benutzerprofil zuzuordnen ist (wer darf mit welchen Programmen auf welche Dateien bzw. Dateisegmente

oder -felder zugreifen?). D. h. detaillierte Zugriffsregelungen zu Programmen und Dateien des Rechenzentrums. Dies ist besonders wichtig im Teilnehmerbetrieb („time-sharing“), in welchem dem Benutzer praktisch alle Betriebsmittel einer DV-Anlage zur Verfügung stehen, um Programme zu entwickeln, auszutesten und Arbeiten durchführen zu lassen.

2.4.5.4 Kontrolle

Die zu beobachtende Entwicklung, daß in zunehmendem Maße eine Dezentralisierung der Datenverarbeitung erfolgt, bringt auch für meine Dienststelle neue Probleme.

Bisher konzentrierte sich die Entwicklung neuer und die Pflege bestehender DV-Verfahren auf die beiden Automationsausschüsse und deren Unterausschüsse. Der Verfahrensablauf – Systementstehungsgang – ist für diese Gremien in den DV-Leitsätzen (DVL) festgelegt. Durch begleitende Beratung in allen Phasen des Systementstehungsganges ist die Rechtmäßigkeit dieser Verfahren in der Regel gewährleistet. Kontrollen bei den sechs Rechenzentren des Verbundes ermöglichen einen Überblick der nach § 10 des Hessischen Datenschutzgesetzes zu treffenden Maßnahmen. Anders die Zukunftsperspektive.

In dem Maße, wie sich Teile von DV-Anwendungen zu den speichernden Stellen verlagern, die entweder über Datenfernverarbeitung auf Verbundrechenzentren zugreifen oder eigene Anlagen der mittleren Datentechnik betreiben, erreichen die durch den Hessischen Datenschutzbeauftragten vorzunehmenden Prüfungen in Qualität und Quantität neue Dimensionen. Es ist nun nicht mehr gewährleistet, daß alle DV-Verfahren in einem vorgeschriebenen Systementstehungsgang entwickelt und freigegeben werden und damit ein Höchstmaß an Transparenz gegeben ist. Außerdem ist festzustellen, daß Entscheidungen über die zu beschaffenden DV-Geräte vorrangig vom Preis/Leistungsverhältnis bestimmt werden, ohne daß z. B. die Leistungsfähigkeit vom Hersteller mitgelieferter Programme (System- und Anwendersoftware) und fest eingebauter Systemkomponenten auf Kriterien des Datenschutzes hin überprüft werden. Meine Erfahrungen haben gezeigt, daß die nach § 10 und der Anlage zu § 10 Abs. 1 S. 1 HDSG zu treffenden organisatorischen und technischen – auch bautechnischen – Maßnahmen oft vernachlässigt werden, soweit sie mit Kosten verbunden sind. Als Fazit bleibt festzuhalten: Es werden zwar Mittel für die

Beschaffung dezentral einzusetzender DV-Anlagen bewilligt, aber Zurückhaltung bei den entsprechenden organisatorischen und technischen Sicherungsmaßnahmen geübt, zumal sich immer wieder herausstellt, daß „Sicherheit“, die nicht vom Hersteller der DV-Geräte mitgeliefert wird, nachträglich mit hohem finanziellen Aufwand durch die speichernden Stellen realisiert werden muß.

2.4.6 Prüfungen bei den Rechenzentren des Hessischen Datenverarbeitungsverbundes

Während des Berichtszeitraumes haben meine Mitarbeiter mit den Rechenzentren des Hessischen DV-Verbundes mehrfach Gespräche geführt und u. a. die Einleitung und Fortschreibung von Maßnahmen nach § 10 HDSG überprüft⁷⁾. Es konnte hierbei von dem in den letzten Jahren erreichten guten Standard ausgegangen werden. Deshalb konzentrierten sich die Überprüfungen auf zwei Schwerpunkte:

1. die Zugangskontrolle, da sich in diesem Bereich immer noch Schwachstellen zeigten und
2. die Zugriffskontrolle, der im Zuge zunehmender Anwendungen im Bereich der Datenfernverarbeitung besondere Bedeutung zugemessen werden muß⁸⁾.

Bei beiden Kontrollen wurden die Anforderungen der „Dienstanweisungen zur Gewährleistung des Datenschutzes und der Datensicherung im Hessischen DV-Verbund (DASCH)“ zugrunde gelegt. Diese Dienstanweisung wurde, wie von mir im Siebenten Tätigkeitsbericht gefordert⁹⁾, den Erfordernissen des Hessischen Datenschutzgesetzes angepaßt und inzwischen durch die Beschlußorgane der jeweiligen Rechenzentren verbindlich eingeführt.

Die Überprüfungen ergaben, daß die von den Kommunalen Gebietsrechenzentren getroffenen organisatorischen und technischen Maßnahmen zur Gewährleistung der Zugangskontrolle zur Zeit ausreichend erscheinen. Die nach § 6 DASCH geforderte Trennung in zwei Sicherheitsbereiche ist durchgeführt, Zugangskontrollen durch besetzte Pforten, Verschluss von Türen und partiellen Einsatz von automatischen Ausweislesern gewährleistet. Restriktive Besucherregelungen, wie Besucherlisten bei dem Pfortner, Ausgabe von

besonderen Besuchermarken, Abholen und Bringen der Besucher von und zur Pforte, ergänzen diese Maßnahmen. Hinzu kommt die Tatsache des „sich gegenseitigen Kennens“ die bei der überschaubaren Größe der Kommunalen Rechenzentren als Schutzeffekt hinzukommt.

Anders stellt sich jedoch die Situation in der Hessischen Zentrale für Datenverarbeitung dar. Die Zugangsregelung an der Pforte ist nur unzureichend. Besucher und Mitarbeiter betreten durch einen gemeinsamen Eingang das Rechenzentrum. Eine Kontrolle wurde insbesondere zu Dienstbeginn und zu Dienstende nur mäßig gehandhabt. Die Trennung von DV-Betrieb (Maschinensaal und Arbeitsvorbereitung) und übrigen Rechenzentrum ist durchgeführt. Der angestrebte Sicherungseffekt tritt aber nicht ein, da grundsätzlich alle im Gebäude verteilten Terminal-Räume unverschlossen und jedem zugänglich sind. Die Verwendung von „Passworten“ beim Terminalbetrieb kann diesen Mangel nicht ausgleichen. Aber auch in anderen Organisationsbereichen des Hauses werden Büroräume während der Abwesenheit der Mitarbeiter nicht verschlossen. Es ist ein leichtes, Datenträger, die unbeaufsichtigt in den Räumen der Organisatoren und Programmierer herumliegen, unbefugt zu entfernen.

Die Hessische Zentrale für Datenverarbeitung steht darüber hinaus vor dem besonderen Problem, daß sich durch umfangreiche Schulungen ständig eine große Anzahl betriebsfremder Personen im Hause aufhalten. Dies gilt entsprechend auch für die sonstigen Besucher, die — durch die Größe des Hauses bedingt — einen zu beachtenden Faktor darstellen.

Es empfiehlt sich deshalb, bei der Realisierung von Maßnahmen der Zu- und Abgangskontrolle nicht nur auf ausschließlich organisatorische Mittel zurückzugreifen. Nach den positiven Erfahrungen der Kommunalen Gebietsrechenzentren mit elektronischen Türschließsystemen auf der Basis von Codierkarten sollte auch dieser Möglichkeit besondere Beachtung gewidmet werden.

Im Bereich der Zugriffssicherung auf Dateien ist dagegen ein erfreulicher Fortschritt zu verzeichnen. Die Hessische Zentrale für Datenverarbeitung, die diese Maßnahmen lange Zeit vernachlässigt hat, ist hier den Kommunalen Gebietsrechenzentren mit gutem Beispiel vorangegangen. Durch massiven und gezielten Einsatz des Datensicherungsprogrammes „SECURE“ ist eine spürbare

⁷⁾ Siehe VII, 12.3.

⁸⁾ Siehe oben, 2.4.5.

⁹⁾ Siehe VII, 12.3.

haltung bei dem Einsatz von „SECURE“ haben dagegen die Kommunalen Gebietsrechenzentren geübt. Teilweise wurden hierfür technische und personelle Engpässe verantwortlich gemacht.

Ich habe in abschließenden Gesprächen mit den Rechenzentren meine Beanstandungen vorgebracht und werde die künftige Entwicklung der zu treffenden Maßnahmen beobachten.

2.5 Praxis der Datenschutzkontrolle

2.5.1 Mitgliederverwaltung für Vereine durch KGRZ

Mehrere hessische Großstädte haben den örtlichen Sportvereinen angeboten, die Mitgliedsbeiträge kostenlos durch das zuständige Kommunale Gebietsrechenzentrum (KGRZ) einziehen zu lassen. Als Gegenleistung wollen sie die persönlichen Daten der Vereinsmitglieder für sportstatistische und Planungszwecke auswerten. Dabei soll ein Erhebungsbogen „Sportvereine – Aufnahmeantrag/Veränderung – Mitgliederstammsatz“ verwendet werden, der bereits die Erklärung der Betroffenen enthält: „Ich bin damit einverstanden, daß meine Daten in einer elektronischen Datenverarbeitungsanlage gespeichert und für Vereinszwecke maschinell ausgewertet werden“. Einzelne Vereine und Bürger haben sich an mich mit der Frage gewendet, ob die Einwilligung in die Datenverarbeitung durch das KGRZ auch die Datenübermittlung an die auftraggebende Stadt umfasse. Sie sahen darin den Datenschutz der Mitglieder gefährdet.

Ich habe die Angelegenheit überprüft und festgestellt, daß es sich dabei nicht um eine öffentliche Aufgabe handelt. Dem kommunalen Automationsausschuß, der sich in seinen Sitzungen am 9. Juli und am 23. Oktober 1979 mit dem Projekt befaßte, habe ich mitgeteilt, daß ich Zweifel an seiner Zuständigkeit in dieser Angelegenheit habe. Es handelt sich bei dem Projekt um eine Datenverarbeitung, die nach dem Dritten Abschnitt des Bundesdatenschutzgesetzes (Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke) zu beurteilen ist. Dabei bedient sich der Verein als speichernde (nicht-öffentliche) Stelle als Auftraggeber der Dienste eines KGRZ, um seinen Mitgliederbestand zu verwalten. Das KGRZ wird als Auftragnehmer im Sinne von § 4 Abs. 1 S. 2 des Gesetzes über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunalen

Abschottung eingetreten. Deutliche Zurück-Gebietsrechenzentren (KGRZ) vom 16. Dezember 1969 (GVBl. I, S. 304) tätig. Der Magistrat der Stadt des Vereinssitzes als öffentliche Stelle im Sinne von § 3 Abs. 1 HDSG kann nicht als speichernde Stelle im Sinne von § 2 Abs. 3 Ziff. 1 HDSG in Frage kommen, denn die Datenverarbeitung von Mitgliedsdaten privater Vereine dient nicht der Erfüllung kommunaler Aufgaben. Auch von seiten des Hessischen Ministers des Innern und des Hessischen Ministers der Finanzen sind insoweit Bedenken geäußert worden.

Aufgrund dieser Rechtsgrundlage findet das Hessische Datenschutzgesetz, das die Datenverarbeitung durch Behörden und öffentliche Stellen des Landes Hessen usw. regelt, keine Anwendung. Soweit das geschilderte Verfahren in Rechenzentren des Verbundes bereits testweise im Einsatz ist, muß die Datenverarbeitung nach dem Dritten Abschnitt des Bundesdatenschutzgesetzes auf ihre Rechtmäßigkeit überprüft werden, und zwar durch den zuständigen Regierungspräsidenten als Datenschutzaufsichtsbehörde für den privaten Bereich.

2.5.2 Steuernummer

In einer Eingabe hatte sich ein Bürger darüber beschwert, daß das für ihn zuständige Finanzamt alljährlich die Aufforderung zur Abgabe einer Einkommenssteuererklärung mit einem Adreßaufkleber versende, der seine Steuernummer offenlege. Er habe auch festgestellt, daß es keine Schwierigkeiten bereite, unter Angabe dieser Steuernummer weitgehende telefonische Auskünfte über die sachlichen und persönlichen Steuerverhältnisse des Steuerpflichtigen zu erhalten, sofern die Befragung geschickt genug erfolge.

Ich habe den Hessischen Minister der Finanzen darauf hingewiesen, daß bei dem geübten Verfahren eine Verletzung des Steuergeheimnisses und der Übermittlungsvorschriften des Hessischen Datenschutzgesetzes nicht auszuschließen sei. Der Hessische Minister der Finanzen hat das beanstandete Verfahren überprüft und mir mitgeteilt, daß künftig der Adreßaufkleber nicht mehr zur Verwendung gelange. Der Versand der Erklärungsvordrucke erfolge mit einem besonderen Einlegeblatt, welches die wichtigsten Steuerdaten des Steuerpflichtigen enthalte. Der Briefumschlag enthalte nur noch die Anschrift.

Das gerügte telefonische Auskunftsverfahren werde durch die hessischen Finanzbehörden

so nicht gehandhabt. Alle Mitarbeiter seien angewiesen, bei telefonischen Anfragen von dem Anrufer Angaben zu erbitten, die nur der Steuerpflichtige oder sein Berater machen könnten. In Zweifelsfällen werde auf die Möglichkeit einer schriftlichen Eingabe verwiesen, oder aber von dem telefonischen Rückruf Gebrauch gemacht.

2.5.3 Neue Abrechnungsnachweise für Beamtengehälter

Die Nachweisung der Gehälter, Vergütungen und Löhne für Bedienstete des Landes Hessen wurde bisher in zwei grundsätzlich verschiedenen Verfahren vorgenommen.

Die Zentrale Vergütungs- und Lohnstelle in Kassel – zuständig für Angestelltenvergütungen und Arbeiterlöhne – versendet an die betroffenen Bediensteten eine Vergütungs- oder Lohnnachweisung, die die Aufschlüsselung der Brutto- bzw. Nettobezüge enthält. Die Nachweisung wird in verdeckter Form in einem ADV-Verfahren gedruckt, d. h. die Außenhülle der Nachweisung ist mit einem geschwärzten Feld versehen und läßt außer der Anschrift keine Entzifferung des Inhalts durch unbefugte Dritte zu. Die dem Verfahren angeschlossenen Kreditinstitute erhalten dann nur noch eine Mitteilung (Girozettel) über die zu überweisende Nettosumme.

Anders das von mir in der Vergangenheit immer wieder kritisierte Verfahren der Besoldungskasse Hessen: Diese teilte den betroffenen Beamten die Festsetzung der Bruttobezüge auf einem besonderen Nachweis mit. Bei der monatlichen Abrechnung des Gehaltes bekamen die angeschlossenen Kreditinstitute offene Gehaltsnachweisungen zugestellt, die außer den Bruttobezügen, die einzelnen Abzüge, wie Lohnsteuer, Kirchensteuer und sonstige freiwillige Abzüge – wie z. B. vermögenswirksame Leistungen – und weitere Angaben über den Gehaltsempfänger enthielten. Die Nachweisungen wurden dann durch die Kreditinstitute den Kontoauszügen des Kontoinhabers beigelegt. Die Vertraulichkeit der personenbezogenen Daten war in diesem Verfahren nicht gewährleistet. Infolge von Rationalisierungsmaßnahmen haben die Kreditinstitute ab 1. Januar 1980 den sog. „beleglosen Datenträgeraustausch“ eingeführt. Auf einem Magnetband werden den Kreditinstituten durch die Besoldungskasse Hessen außer den Kontendaten des Gehaltsempfängers nur noch die zu überweisende Nettosumme mitgeteilt. Die Nachweisung des aufgeschlüsselten Gehaltes erfolgt künftig in

ähnlicher Weise wie bei der Zentralen Vergütungs- und Lohnstelle. D. h. der betroffene Beamte erhält seine Abrechnungsnachweise in einem verdeckten Blatt direkt von der Besoldungskasse Hessen über seine Beschäftigungsbehörde.

Damit ist weitgehend sichergestellt, daß eine unzulässige Übermittlung von Gehaltsdaten nicht mehr erfolgt.

2.6 Datenschutz im kirchlichen Bereich

2.6.1 Prüfungsvoraussetzungen

Im Siebenten Tätigkeitsbericht (1., S. 48) habe ich dargelegt, welche verfassungsrechtlichen Gesichtspunkte bei der Datenübermittlung aus dem öffentlichen Bereich an öffentlich-rechtliche Religionsgesellschaften (§ 12 Abs. 1 HDSG – § 10 Abs. 1 BDSG) zu beachten sind:

Die Bindung staatlicher Gewalt an die Grundrechte und der Grundsatz der Trennung von Staat und Kirche (Art. 48 Abs. 3 HV, Art. 140 GG i. V. m. Art. 137 Abs. 1 WRV) setzen der entsprechenden Anwendung der Vorschriften über die Datenübermittlung innerhalb des öffentlichen Bereichs zusätzliche Schranken. Dabei habe ich die Frage offengelassen, ob sichergestellt ist, daß bei den Religionsgesellschaften ausreichende Datenschutzmaßnahmen getroffen worden sind.

Die nunmehr vorgenommene Überprüfung der kirchenrechtlichen Vorschriften hat ergeben, daß der Datenschutz innerhalb der beiden Kirchen rechtlich gewährleistet ist.

2.6.1.1 Es stellte sich zunächst die Frage, welche Kriterien dafür zu gelten haben, ob die öffentlich-rechtliche Religionsgesellschaft als Empfänger personenbezogener Daten aus dem staatlichen Bereich ausreichende Maßnahmen für den Datenschutz getroffen hat. Als Maßstab hierfür bietet sich die staatliche Datenschutzregelung an. Sichert die Regelung der Religionsgesellschaften den gleichen oder einen gleichwertigen Datenschutz wie der Staat, so ist die gesetzliche Voraussetzung für die Zulässigkeit der Datenübermittlung an sie erfüllt. Strengere Anforderungen können an die Religionsgesellschaften nicht gestellt werden; anderenfalls würde die staatliche Regelung als unzureichend qualifiziert werden; denn es kann nicht unterstellt werden, daß die Gefährdung der schutzwürdigen Belange des Betroffenen im kirchlichen Bereich größer ist als im staatlichen, und daß deswegen strengere

Datenschutzvorkehrungen nötig sind. Andererseits kann die Frage, ob und inwieweit Datenschutzregelungen der Religionsgesellschaft noch als ausreichend zu beurteilen sind, wenn sie hinter den Anforderungen der staatlichen Datenschutzgesetze zurückbleiben, nicht in gleicher Weise allgemein, sondern nur aufgrund der konkreten Vorschriften und unter Berücksichtigung der Besonderheiten, die sich aus der Zugehörigkeit des Betroffenen zu einer Religionsgesellschaft ergeben können, beantwortet werden.

2.6.1.2 Der nach diesen Maßstäben durchgeführten Prüfung liegen zugrunde:

- a) Das Kirchengesetz über den Datenschutz vom 10. November 1977, das die Synode der Evangelischen Kirche in Deutschland aufgrund von Art. 10 b der Grundordnung beschlossen hat und das am 1. Januar 1978 in Kraft getreten ist (vgl. Anlage I Abschn. I: unten 3.1).

Das Kirchengesetz der EKD ist von den evangelischen Gliedkirchen im Lande Hessen, nämlich den Evangelischen Kirchen in Hessen und Nassau, in Kurhessen-Waldeck und im Rheinland übernommen worden.

- b) Die Durchführungsverordnung der Evangelischen Kirche im Rheinland vom 11. Mai 1978 (vgl. Anlage I Abschn. II: unten 3.1).

„Mit geringen Ausnahmen gleichlautende Rechtsverordnungen zum Kirchengesetz über den Datenschutz (Datenschutzverordnungen) haben die Evangelische Kirche in Hessen und Nassau am 21. Dezember 1979 (ABl. Nr. 13 S. 34 f.) und die Evangelische Kirche von Kurhessen-Waldeck am 30. Oktober 1979 (ABl. 1980, Nr. 1 S. 21 ff.) erlassen.“ Die Abweichungen von der Durchführungsverordnung der Evangelischen Kirche im Rheinland sind für die hier untersuchte Frage ohne Bedeutung.

- c) Die gleichlautenden Anordnungen über den kirchlichen Datenschutz (KDO) der Diözesen Fulda, Limburg, Mainz und der Erzdiözese Paderborn (vgl. Anlage II: unten 3.1).

2.6.1.3 (Exkurs) Nach dem mir bisher bekanntgewordenen Stand haben noch folgende weitere Gliedkirchen der EKD innerhalb der Bundes-

republik Deutschland das Kirchengesetz der EKD übernommen:

- Die Evangelisch-Lutherische Kirche in Bayern (Kirchliches Datenschutzdurchführungsgesetz vom 4. Dezember 1978 - ABl. S. 348),
- die Evangelisch-Lutherische Landeskirche von Braunschweig (Kirchengesetz vom 10. Dezember 1977 - ABl. 1978 S. 19),
- die Evangelisch-Lutherische Landeskirche Hannover (Datenschutzanwendungsgesetz vom 7. Dezember 1977 - ABl. S. 166),
- die Lippische Landeskirche (Fundstelle unbekannt); sie hat zur Durchführung des EKD-Gesetzes eine Durchführungsverordnung vom 5. Juli 1978 (Abl. der EKD 1979 S. 65 ff.) erlassen, die mit der Durchführungsverordnung der EK im Rheinland vom 11. Mai 1978 übereinstimmt,
- die Evangelisch-Reformierte Kirche in Nord-West-Deutschland (Kirchengesetz vom 25. November 1977 - GVBl. S. 296),
- die Evangelisch-Lutherische Kirche in Oldenburg (Kirchengesetz vom 24. November 1977 - GVBl. S. 41),
- die Evangelische Kirche der Pfalz (Beschluß der Landessynode vom 26. April 1978 - ABl. S. 71),
- die Evangelische Landeskirche Schaumburg-Lippe (Beschluß des Landeskirchenrates vom 26. November 1977 - ABl. Nr. 2),
- die Evangelische Kirche von Westfalen (Datenschutzordnung vom 3. November 1978 - ABl. S. 160 - mit der Durchführungsverordnung vom 23. Januar 1979 - ABl. S. 44 -, die mit der Durchführungsverordnung der EK im Rheinland vom 11. Mai 1978 übereinstimmt.

2.6.2 Der Datenschutz in der Evangelischen Kirche in Hessen

Wie die - als Anlage I beigefügte - Übersicht (Abschn. I: unten 3.1) zeigt, gleichen die Regelungen des EKD-Gesetzes denjenigen der staatlichen Gesetze.

2.6.2.1 Das EKD-Gesetz enthält zwar nur einige Grundsätze des Datenschutzes, die allein

keinen dem staatlichen Datenschutzrecht vergleichbaren Datenschutz gewähren. Solange die in § 10 Abs. 1 S. 1 vorgesehenen Rechtsverordnungen des Rates der EKD fehlt, und soweit die Gliedkirchen den ihnen in § 10 Abs. 1 S. 1 erteilten Auftrag, die nötigen Ergänzungs- und Durchführungsbestimmungen zu erlassen, nicht erfüllt haben, sind jedoch die „bundesrechtlichen Bestimmungen“ zur Ausfüllung der Lücken in entsprechender Anwendung heranzuziehen (§ 10 Abs. 2, vgl. Anlage I Abschn. I). Mit dieser die Kirchengesetze ergänzenden Einbeziehung der bundesrechtlichen Bestimmung über den Datenschutz, die sich nicht auf das Bundesdatenschutzgesetz beschränken, sondern das gesamte Bundesrecht, soweit es Datenschutzbestimmungen enthält, einbezieht, sichert die kirchengesetzliche Regelung einem dem staatlichen Recht gleichwertigen und somit ausreichenden Datenschutz.

Die Verweisung auf die bundesrechtlichen Datenschutzvorschriften – und nicht auf die für die Gliedkirchen in Betracht kommenden landesrechtlichen Vorschriften – ist aus dem räumlichen Geltungsbereich des EKD-Gesetzes zu erklären. Für den Umfang des Datenschutzes im Lande Hessen entstehen daraus keine Folgerungen, weil das HDSG das BDSG – von einigen hier nicht einschlägigen Abweichungen abgesehen – übernommen hat.

2.6.2.2 Der Vergleich der Durchführungsverordnung der Evangelischen Kirche im Rheinland vom 11. Mai 1978 (Abschn. II der Anlage I) mit dem staatlichen Datenschutzrecht erweist eine weitgehende Übereinstimmung. Die Abweichungen erklären sich aus der Verschiedenartigkeit der Aufgaben, die dem Staat und die der Kirche gestellt sind.

2.6.3 Der Datenschutz in der Katholischen Kirche in Hessen

2.6.3.1 Für den Bereich der Katholischen Kirche in Hessen ist der Datenschutz in gleichlautenden bischöflichen Gesetzen für die Diözesen Fulda, Limburg, Mainz und Paderborn geregelt. Diese „Anordnungen über den kirchlichen Datenschutz – KDO“ stimmen in ihrem Aufbau und in ihrem Wortlaut mit dem BDSG überein, soweit nicht der Unterschied zwischen der staatlichen und der kirchlichen Behördenorganisation und das „Spezifikum des geistig-religiösen Auftrags der Kirche“ (BVerfGE 42, 312 ff.) Abweichungen gebietet. Vgl. die als Anlage II beigefügte Gegen-

überstellung des Textes des BDSG und der Abweichungen der KDO (siehe unten 3.2.).

2.6.3.2 Demgemäß gelten die Anordnungen für personenbezogene Daten, die „vom Bistum, von den Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbänden und von ihrer Aufsicht unterstehenden kirchlichen Körperschaften, Stiftungen, Anstalten, Werken und Einrichtungen sowie im Auftrag dieser Stellen in Dateien verarbeitet werden (§ 1 Abs. 2 KDO)“.

Nach § 1 Abs. 3 KDO gehen besondere kirchliche oder staatliche Rechtsvorschriften, soweit sie auf die Dateien gespeicherte personenbezogene Daten anzuwenden sind, den Vorschriften der KDO vor. Diese Vorschrift entspricht § 45 S. 1 BDSG.

Nach § 1 Abs. 4 KDO bleiben unberührt die Verpflichtung zur Verschwiegenheit über die in Ausübung priesterlicher oder seelsorglicher Tätigkeit erworbenen Kenntnisse über persönliche Angelegenheiten dritter Personen und die dienstliche Schweigepflicht. Diese Regelung entspricht dem § 45 S. 2 Nr. 1 BDSG.

Im Kirchengesetz der EKD über den Datenschutz (vgl. Anlage I-Nr. 3) ist in § 1 Abs. 3 dem Pfarrer und den kirchlichen Mitarbeitern das Recht zugebilligt, in Wahrnehmung ihres Seelsorgeauftrags über ihren Dienst an Kirchenmitgliedern eigene Aufzeichnungen zu führen und zu verwenden. Dort ist ausdrücklich erlaubt, was hier nur zulässig ist, wenn die KDO oder eine staatliche oder andere kirchliche Rechtsvorschrift es gestattet (§ 7 KDO).

Abweichend von dem EKD-Gesetz über den Datenschutz verwendet die KDO als Mittel des Datenschutzes das Verbot der Datenverarbeitung mit dem Vorbehalt der Erlaubnis wie das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder. Danach ist die Verarbeitung personenbezogener Daten im kirchlichen Bereich nur zulässig, wenn die KDO, eine andere kirchliche Rechtsvorschrift oder eine staatliche Rechtsvorschrift sie erlaubt oder wenn der Betroffene eingewilligt hat (§ 7).

Auch in diesem Falle scheint es der grundsätzlichen Ausgliederung der eigenen Angelegenheiten der Kirche aus der Bindung an staatliche Gesetze zu widersprechen, daß die KDO es auch einer staatlichen Rechtsvorschrift vorbehält, die Datenverarbeitung im

kirchlichen Bereich zuzulassen. Da die Verarbeitung von Daten ein vornehmlich technisches Mittel der Sammlung, Aufbereitung und Weiterleitung von Informationen darstellt, ist es aber nur schwer vorstellbar, daß ein staatliches Gesetz der Kirche vorschreiben könnte, in ihren eigenen Angelegenheiten und zur Person ihrer Mitglieder gesammelte Daten nicht oder nur unter bestimmten Voraussetzungen zu verarbeiten. Eine solche staatliche Rechtsvorschrift müßte jedenfalls ein für alle geltendes Gesetz sein.

Die Datenübermittlung im kirchlichen Bereich regelt § 10 KDO:

Im ersten Absatz wird die Übermittlung innerhalb des in § 1 Abs. 2 festgelegten Geltungsbereich der KDO ebenso wie in § 1 Abs. 2 Nr. 1 BDSG geregelt.

Der zweite Absatz betrifft die Übermittlung an **kirchliche Werke und Einrichtungen**, die nicht unter § 1 Abs. 2 KDO fallen. Welche einzelnen Werke und Einrichtungen dies sind, läßt das Kirchengesetz nicht erkennen. Auch in den ergänzenden Anordnungen und Ausführungsbestimmungen zum kirchlichen Datenschutz und kirchlichen Meldewesen vom 9. April 1979 (ABl. der Diözese Fulda Nr. IV vom 26. April 1979 Nr. 80) sind als speichernde Stellen neben dem Bistum, den Kirchengemeinden etc. – wie in § 1 Abs. 2 KDO – aufgeführt: „Werke und Einrichtungen, die der Aufsicht des Bistums und der Kirchengemeinde unterstehen“. Demnach ist die Unterstellung unter die Aufsicht des Bistums oder einer Kirchengemeinde das Unterscheidungsmerkmal mit der Folge, daß kirchliche Werke und Einrichtungen, die dieser Aufsicht nicht unterstehen, zwar zum kirchlichen Bereich gehören, im übrigen aber von der KDO nur erfaßt werden, soweit personenbezogene Daten an sie übermittelt werden: Die Zulässigkeit der Datenübermittlung an „Werke und Einrichtungen“, die nicht der kirchlichen Aufsicht unterstehen, ist davon abhängig, daß der Empfänger sich verpflichtet, die KDO hinsichtlich der zu empfangenden Daten anzuwenden, Weisungen der übermittelnden Stelle einzuhalten und sich der Aufsicht des kirchlichen Datenschutzbeauftragten zu unterstellen. Dem Empfänger ist ferner die Übermittlung der empfangenden Daten an andere Stellen untersagt. Dies entspricht der Regelung, die das HDSG in § 4 Abs. 1 S. 3 für die Verarbeitung von Daten im Auftrage der Behörden durch Stellen, die dem Datenschutzgesetz nicht unterstehen, vorschreibt.

Die Übermittlung personenbezogener Daten an Stellen **anderer öffentlich-rechtlicher Religionsgesellschaften** ist nach Abs. 3 in entsprechender Anwendung von Abs. 1 zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden und staatliche Rechtsvorschriften dem nicht entgegenstehen.

In gleicher Weise regelt Abs. 4 die Übermittlung personenbezogener Daten an **Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Kommunen etc.** Die Übermittlung ist in entsprechender Anwendung von Abs. 1 nur zulässig, soweit es nach staatlichem Recht erlaubt ist und kirchliche Datenschutzbestimmungen dem nicht entgegenstehen.

In beiden Fällen der Abs. 3 und 4 werden Einwirkungen aus der staatlichen Rechtsordnung in den kirchlichen Bereich zugelassen. Der Vorbehalt der staatlichen Erlaubnis umfaßt die gesamte staatliche Rechtsordnung. Die Übermittlung personenbezogener Daten aus dem kirchlichen Bereich heraus ist dadurch in doppelter Weise gesichert: Die Übermittlung muß nach dem staatlichen Recht des Empfängers erlaubt und nach den kirchlichen Datenschutzbestimmungen zulässig sein. In dieser Hinsicht kann die Bindung des Staates an das Grundrecht des Art. 4 GG zum Tragen kommen.

Die Übermittlung „außerhalb des kirchlichen und öffentlichen Bereiches“ (§ 11), d. h. die Übermittlung an Einzelpersonen oder an andere privatrechtliche Stellen ist in gleicher Weise wie die Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs in § 11 S. 1 BDSG geregelt.

Die weiteren Vorschriften der KDO entsprechen den Vorschriften des Ersten und Zweiten Abschnitts des BDSG.

2.6.4 Kirchliches Meldewesen

- 2.6.4.1 Bevor das Kirchengesetz der EKD über den Datenschutz vom 10. November 1977 und die übereinstimmenden Anordnungen der Diözesen über den kirchlichen Datenschutz (KDO) verkündet waren, galten in beiden Kirchen Datenschutzregelungen aufgrund des Kirchengesetzes der EKD über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder vom 10. November 1976 und aufgrund übereinstimmender Anordnungen der Diözesen über das kirchliche Meldewesen (KMAO) aus dem Jahre 1978. Das Kirchengesetz der EKD

einschließlich der Ausführungsverordnungen der Gliedkirchen sowie die Anordnungen der katholischen Bischöfe über den kirchlichen Datenschutz enthalten keine Vorschriften über ihr Verhältnis zu den vorgenannten Bestimmungen über das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder. Es liegt nahe anzunehmen, daß die Vorschriften über das kirchliche Meldewesen insgesamt als eine spezielle kirchenrechtliche Regelung zu verstehen sind, die einer bereichsspezifischen Regelung im staatlichen Recht in bezug auf das Melderecht entspricht, und demgemäß als Spezialvorschrift dem allgemeinen Datenschutzrecht in den Kirchen vorgeht bzw. es ergänzt.

2.6.4.2 Inhaltlich stimmen die Anordnungen für das Meldewesen mit den Vorschriften der allgemeinen Datenschutzgesetze bzw. -anordnungen überein:

Jede Kirchengemeinde ist verpflichtet, ein Verzeichnis der Kirchenmitglieder zu führen (Gemeindemitgliederverzeichnis). Das Gemeindemitgliederverzeichnis enthält die Daten der Kirchenmitglieder und ihrer Familienangehörigen (Familienverbund). Diese Daten sind zu berichtigen, wenn sie unrichtig sind oder unrichtig werden. Demgemäß wird das Kirchenmitglied verpflichtet, die Begründung eines neuen oder eines weiteren Wohnsitzes bei den zuständigen kirchlichen Stellen anzu-melden.

Hierzu enthält § 16 des Kirchengesetzes über die Kirchenmitgliedschaft der EKD vom 10. November 1976 folgende bemerkenswerte Bestimmungen:

Nach Abs. 1 S. 2 ist der Meldepflicht gegenüber der kirchlichen Stelle genügt, wenn sich das Kirchenmitglied unter Angabe der Religionszugehörigkeit bei der staatlichen oder kommunalen Meldebehörde anmeldet; und nach Abs. 2 fordern die kirchlichen Stellen die Meldedaten von dem Kirchenmitglied nur an, wenn sie die Daten von den staatlichen oder kommunalen Meldebehörden, von der Kirchengemeinde des früheren Wohnsitzes oder aus eigenen Unterlagen nicht oder nur unvollständig erhalten.

Die evangelische Kirche setzt offensichtlich einen ungehinderten Datenfluß zwischen den staatlichen Meldebehörden und den kirchlichen Stellen voraus. Soweit das Verfahren auch auf die der Kirche nicht angehörenden Familienangehörigen (Familienverbund) bezogen wird, widerspricht es jedoch der Bin-

dung der staatlichen und der kommunalen Behörden an die Grundrechte der Verfassung (vgl. oben 6.1 und die verfassungsrechtliche Darlegung im 11. Abschnitt des Siebenten Tätigkeitsberichtes). Darüber hinaus läßt die kirchenrechtliche Regelung die Pflicht der Behörden und öffentlichen Stellen, personenbezogene Daten unter den Voraussetzungen des § 19 Abs. 2 HDSG zu sperren sowie die Rechte des Betroffenen, die Sperrung seiner Daten nach § 8 Abs. 1 Nr. 3 HDSG oder nach § 16 a Abs. 4 des Hessischen Meldegesetzes zu verlangen, unberührt.

2.6.4.3 Bezüglich der Datennutzung (Datenweitergabe) sind die kirchlichen Meldebehörden berechtigt, den zuständigen kirchlichen Stellen die zur Wahrnehmung der Aufgaben der Kirchen erforderlichen Daten zur Verfügung zu stellen.

An „Werke und Einrichtungen“ der Evangelischen Kirche können die Meldedaten insoweit weitergegeben werden, als die Werke und Einrichtungen für die Erfüllung des Auftrages der Kirche in den Gliedkirchen verantwortlich sind (§ 15 Ab. 2 des Kirchengesetzes über die Kirchenmitgliedschaft).

In der Anordnung der Diözesen (KMAO) fehlt eine entsprechende Vorschrift. Jedoch enthält die KMAO die Vorschrift, daß Meldedaten an juristische Personen des Privatrechts insoweit weitergegeben werden können, als diese „für die Erfüllung kirchlicher Aufgaben zuständig“ sind (§ 5 Abs. 2 KMAO). Im übrigen ist vorgesehen, daß das Verfahren der Datenweitergabe bzw. die Einhaltung der Zweckbestimmung der Datenspeicherung durch besondere bischöfliche Anordnungen bzw. durch das Recht der Gliedkirchen geregelt wird.

Diese Regelungen enthalten nunmehr die Anordnung über den kirchlichen Datenschutz (KDO) und das EKD-Gesetz über den Datenschutz mit den dazugehörigen Ergänzungs- und Ausführungsbestimmungen der Gliedkirchen. Das gleiche gilt für den von beiden Kirchen aufgestellten Grundsatz, daß der für die Erfüllung des Auftrages der Kirche erforderliche Datenaustausch zu gewährleisten ist, und daß dabei jede kirchliche Stelle die in den Gemeindemitgliederverzeichnissen enthaltenen persönlichen Daten der Kirchenmitglieder gegen Mißbrauch zu schützen hat.

Die Weitergabe der Daten ist nur zulässig, wenn sichergestellt ist, daß auch bei dem Empfänger ausreichende Maßnahmen gegen

den Mißbrauch der Daten getroffen worden sind (vgl. §§ 17 und 18 des Kirchengesetzes über die Kirchenmitgliedschaft vom 10. November 1978 und §§ 7 und 8 der Kirchenmeldewesenverordnung - KMAO -).

2.7 Bereichsspezifische Regelungen

2.7.1 Personalausweisgesetz

Im März des Berichtsjahres habe ich im Rahmen meiner Beratungskompetenz die Landesregierung auf die Bedenklichkeit des § 2 Abs. 2 Personalausweisgesetz hingewiesen. Meine Prüfung wurde angeregt durch eine Meldung in einer regionalen Anzeigenzeitung, die einen Bürger zu einer Eingabe veranlaßt hatte. Dort wurde berichtet: Künftig wird jeder Bundesbürger für jedermann einsehbar sein Strafregister mit sich herumtragen: Mit einem Blick in den Personalausweis wird man feststellen können, daß sein Inhaber bei der Polizei „aktenkundig“ ist. Seit einigen Wochen sind nämlich die Meldebehörden dazu übergegangen, vor Verlängerung oder Neuausstellung eines Personalausweises bei der Polizei anzufragen, ob beim Polizeicomputer in Wiesbaden etwas vorliegt. Ist der Antragsteller dort registriert, bringt der Sachbearbeiter auf der Seite 2 des Ausweises in der Rubrik „unveränderliche Kennzeichen“ einen Stempel an. Auf die Seite 8 kommt ein zweiter Stempel mit dem Text § 2 Abs. 2 PAG“, der dann jedem kundtut, daß der Inhaber des Ausweises sich in den Maschen des Gesetzes verfangen hat.

Die Überprüfung der Sach- und Rechtslage hat folgendes ergeben:

Der Bundesgesetzgeber hat durch das Gesetz zur Änderung des Gesetzes über Personalausweise und zur Regelung der Meldepflicht in Beherbergungsstätten vom 6. November 1978 (BGBl. I S. 1712) folgenden Abs. 2 an § 2 des Personalausweisgesetzes angefügt:

(2) Unter den Voraussetzungen des § 7 Abs. 1 des Gesetzes über das Paßwesen kann die zuständige Behörde im Einzelfall anordnen, daß der Personalausweis abweichend von den Bestimmungen einer Rechtsverordnung nach § 3 Abs. 1 des Gesetzes über das Paßwesen nicht zum Verlassen des Gebietes des Geltungsbereichs des Grundgesetzes (einschließlich des Gebietes des Landes Berlin) über eine Auslandsgrenze berechtigt. Der Inhaber des Personalausweises ist verpflichtet, diesen zur Anbringung eines Vermerks über die Anordnung nach Satz 1 der zuständigen Behörde vorzulegen.

Der Zweck der Änderung wird in der Durchführungsverordnung des Hessischen Ministers des Innern, Az.: III A 52 - 23 c 10, StAnz. Nr. 49/1978 S. 2389, erläutert: Durch diese Vorschrift ist die Möglichkeit eröffnet worden, Personen, gegen die Paßversagungsgründe vorliegen, auch dann an der Ausreise aus dem Bundesgebiet in das Ausland zu hindern, wenn für den Grenzübertritt ein Personalausweis ausreicht. Damit ist dem Mangel abgeholfen worden, der darin bestand, daß nach bisherigem Recht bei Versagen eines Passes gleichwohl ein Verlassen des Bundesgebietes mit einem Personalausweis möglich war. Der den Grenzübertritt verhindernde Vermerk wird auf der für amtliche Vermerke vorgesehenen Seite 8 des Personalausweises in folgender Fassung eingetragen: § 2 Abs. 2 Personalausweisgesetz. Dazu heißt es weiter in der Vorschrift: Um die Aufmerksamkeit eines den Ausweis kontrollierenden Beamten auf das Vorhandensein einer solchen Eintragung auf Seite 8 des Personalausweises hinzuweisen, ist auf Seite 2 des Ausweises am rechten unteren Rand der Spalte „unveränderliche Kennzeichen“ ebenfalls der Abdruck eines Dienstsiegels anzubringen.

Diese Regelung gab verfassungsrechtlich besonders unter Datenschutzaspekten in mehrfacher Hinsicht zu Bedenken Anlaß. Der Betroffene wurde aufgrund des Personalausweisgesetzes i. V. m. dem Hessischen Ausführungsgesetz zum Personalausweisgesetz und eines darauf beruhenden Erlasses gezwungen, gegenüber jedermann, der aus öffentlich-rechtlichem, geschäftlichem oder privatem Anlaß die Vorlage des Personalausweises zur Legitimation bzw. Identifikation verlangt, die im Melderegister über ihn vermerkte Tatsache der Paßversagung zu offenbaren. Dieser Offenbarungszwang gegenüber potentiell jedermann ist die Konsequenz aus der gesetzlichen Verpflichtung jeder meldepflichtigen Person über 16 Jahren der Bundesrepublik, einen Personalausweis zu besitzen.

Zweck des Personalausweises ist der Nachweis der Identität im Inland (vgl. § 1 Abs. 1 PAG „zur Prüfung der Personalien“; BVerwG U. vom 4. Juli 1972 - I c 7/71). Durch § 1 Ziff. 4 und 5 der Durchführungsverordnung zum Paßgesetz vom 29. Januar 1969 ist der Paßzwang im Verkehr mit bestimmten Staaten aufgehoben worden. Dadurch ist der Personalausweis aufgrund einer Verordnung zum Paßgesetz dem Reisepaß als Grenzdokument partiell gleichgestellt worden. Der Gesetzgeber hat nun aus dieser teilweisen funktionalen

Äquivalenz der Personaldokumente versucht, die Regelung über die Paßversagung auf das Personalausweisgesetz zu übertragen. Die Paßversagung hat den ausschließlichen Zweck, die Ausreise aus der Bundesrepublik zu verhindern. Dem Paßbewerber kann bei dem begründeten Verdacht, daß Paßversagungsgründe gemäß § 7 Abs. 1 Paßgesetz vorliegen, der Paß versagt, dem Inhaber eines gültigen Passes unter Voraussetzung des § 7 Abs. 1 der Paß entzogen werden. Eine Pflicht für jeden Deutschen, einen Paß zu besitzen, besteht nicht. Zur inländischen Personalfeststellung kann der Reisepaß aber hilfsweise dienen (vgl. § 1 Abs. 1 Personalausweisgesetz). Für niemanden außerhalb der zuständigen Behörden wurde daher die Tatsache der Paßversagung im Inland offenbart, wenn der Betreffende durch gültigen Personalausweis identifiziert werden konnte. Die Paßversagung stand daher in einem angemessenen Verhältnis zu dem Zweck, der erreicht werden sollte, nämlich der Verhinderung der Ausreise.

Der Eingriff des Gesetzgebers durch § 2 Abs. 2 Personalausweisgesetz in die allgemeine Handlungsfreiheit war meiner Auffassung nach unverhältnismäßig und verletzte das verfassungsrechtliche Übermaßverbot. Das Recht auf Ausreise ist nach der ständigen Rechtsprechung des Bundesverfassungsgerichts (vgl. Entscheidungen 632ff.) verfassungsrechtlich in der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 verankert. Diese allgemeine Handlungsfreiheit ist durch die Schranke der verfassungsmäßigen Ordnung nur im Rahmen aller formell und materiell gültig zustande gekommener Gesetze einschränkbar. § 7 Paßgesetz ist in diesem Zusammenhang vom Bundesverfassungsgericht als Teil der verfassungsmäßigen Rechtsordnung und damit als verfassungskonform angesehen worden.

§ 2 Abs. 2 Personalausweisgesetz allerdings greift wesentlich weiter in die allgemeine Handlungsfreiheit ein. Bei der Regelung des § 7 Paßgesetz wurde in die allgemeine Handlungsfreiheit nur insoweit eingegriffen, als es zur Verhinderung der Ausreise erforderlich war. Durch die Verpflichtung zum Besitz eines Personalausweises und durch die neue Regelung, die einen für jedermann erkenntlichen Vermerk über die Tatsache der Paßversagung vorschreibt, wurde der Betroffene gegen seinen Willen gezwungen, dieses Datum jedem, mit dem er im Inland in behördlichen oder geschäftlichen Verkehr trat, zu offenbaren,

ohne daß diese allgemeine Stigmatisierung zur Verhinderung der Ausreise erforderlich oder gar zweckmäßig gewesen wäre. Darüber hinaus ist die Regelung rechtsstaatlich höchst bedenklich, weil sie unbefugten Dritten eine vage Information über den Betroffenen vermittelt, die schon im Ansatz der Zuverlässigkeit eines rechtskräftigen Urteils oder Verwaltungsaktes entbehrt: Der Bürger oder Beamte, dem der Betroffene einen solchermaßen gekennzeichneten Ausweis vorlegt, erkennt, daß sein Gegenüber verdächtig wird, zum Beispiel ein Verfassungsfeind zu sein, eine Straftat begangen zu haben, Steuern zu hinterziehen, seiner gesetzlichen Unterhaltspflicht nicht nachzukommen oder gar zu desertieren.

Hier würde für jedermann offenbart, was im jeweiligen spezialgesetzlichen Bereich strengsten Geheimhaltungs- und Übermittlungsvorschriften, sogar im Behördenverkehr, unterliegt.

Eine solche Stigmatisierung verstößt gegen das Rechtsstaatsgebot des Grundgesetzes und das Verbot der Brandmarkung in Artikel 3 der Menschenrechtskonvention und Artikel 9 der UN-Charta. Darüber hinaus führt eine Einbeziehung des Wertgehalts von Art. 1 Abs. 1 des Grundgesetzes (GG) in das Hauptfreiheitsrecht des Art. 2 Abs. 1 GG zu einem allgemeinen Persönlichkeitsrecht mit Grundrechtsqualität (vgl. Maunz/Dürig/Herzog/Scholz, Art. 1 Abs. 1 GG, Rdnr. 37 ff; BVerfGE 6, 41; 6, 433), an dem staatliches Handeln seine Grenze findet. Das allgemeine Persönlichkeitsrecht umfaßt alle Einzelrechte, deren Garantie es bedarf, um zu verhindern, daß der einzelne Machtansprüchen Dritter oder der Gemeinschaft wegen unterworfen wird. Alle Staatsgewalt hat den Menschen in seinem Eigenwert, seiner Eigenständigkeit zu achten und zu schützen. Er darf nicht „unpersönlich“, nicht wie ein Gegenstand behandelt werden, auch wenn es nicht aus Mißachtung des Personenwertes, sondern „in guter Absicht“ geschieht (vgl. BVerfG 30, 40). Gegen diesen Grundsatz wird durch die Regelung des § 2 Abs. 2 Personalausweisgesetz in eklatanter Weise verstoßen. § 2 Abs. 2 ist daher unverhältnismäßig, weil der Eingriff in die allgemeine Handlungsfreiheit und das Persönlichkeitsrecht gegen das Übermaßgebot verstößt. Der staatliche Zweck läßt sich mit geringeren Eingriffen in die Grundrechtsposition des Bürgers ebenso sicherstellen. In diesem Zusammenhang bleibt zu bemerken, daß ein so bekannter Kommentator wie Dürig

bereits dann einen Verstoß gegen Art. 1 Abs. 1 GG unterstellt, wenn auf Personalausweisen Fingerabdrücke nach der Regelung des Personalausweisgesetzes von 1937 beibehalten worden wären. Er wertet eine solche Kennzeichnung als staatliche Maßnahme zur „Entpersönlichung des einzelnen“ (vgl. Maunz/Dürig/Herzog/Scholz Art. 1 Abs. 1 Rdnr. 37f.).

Obendrein war die Ausgestaltung des Verwaltungsverfahrens durch die Verordnungsermächtigung nicht gedeckt. Der Zweck des Personalausweises ist die Identifikation der Person. Form und Inhalt des Personalausweises müssen nicht vollständig durch das Gesetz selbst bestimmt werden. Es genügt, daß § 1 Abs. 1 Personalausweisgesetz den Zweck des Personalausweises festlegt, Abs. 2 ein einheitliches Muster mit Raum für ein Lichtbild vorschreibt, in dem Raum für einen Fingerabdruck nicht vorgesehen werden darf. Hinweise auf den Verdacht einer Straftat, verfassungsfeindlicher Tätigkeit, Steuerhinterziehung oder Desertion dienen aber nicht zur Beschreibung einer Person. Damit überschreitet § 2 Abs. 2 und die dazugehörige Verwaltungsvorschrift den Regelungsbereich des Personalausweisgesetzes. Das Anbringen eines Dienstsiegels in der Rubrik „unveränderliche Kennzeichen“ mit der Funktion eines Hinweises auf einen Vermerk auf Seite 8 des Personalausweises wird von Grund und Zweck der Spalte „unveränderliche Kennzeichen“, die zusammen mit dem Lichtbild der äußerlichen Identifikation dienen soll, nicht gedeckt. Delikaterweise stehen unter Umständen sich nicht als begründet erweisende Verdachtsmomente, symbolisiert durch ein Dienstsiegel, unter einer Rubrik, die immerhin eine unveränderliche, d. h. dauernde, Kennzeichnung einer Person darstellen.

Der hessische Ausführungserlaß war infolgedessen nicht vom Personalausweisgesetz gedeckt. Die konkrete Ausgestaltung verstieß gegen das Rechtsstaatsgebot, griff unverhältnismäßig und im Übermaß in die allgemeine Handlungsfreiheit des Betroffenen ein und verletzt den Kernbereich des Persönlichkeitsrechts gemäß Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG.

Der sog. „Säuferbalken“ im Führerschein, der eine wesentliche harmlosere Information enthielt, war bereits aus rechtsstaatlichen und datenschutzrechtlichen Gesichtspunkten heraus abgeschafft worden; die Stigmatisierung eines Verdächtigen im Sinne der §§ 7 Abs. 1 Paßgesetz i. V. m. 2 Abs. 2 Personalausweis-

gesetz ist mit dem konstituierenden Prinzip des Grundgesetzes, dem Schutz und der Wahrung der Menschenwürde durch die öffentliche Verwaltung unvereinbar. Ich habe bei allen diesen Erwägungen nicht übersehen, daß eine Reihe wichtiger Gründe für gesetzliche und administrative Vorkehrungen sprechen können, die es ermöglichen, die Ausreise aus der Bundesrepublik zu unterbinden. Insofern sind die Motive des Gesetzgebers zu § 2 Abs. 2 Personalausweisgesetz einsichtig und für jedermann plausibel. Es gehört aber nun einmal zu den politischen Kosten des Rechtsstaats, nicht die auf den ersten Blick vielleicht praktikabel anmutende Maßnahme zu ergreifen, sondern diejenige Form staatlichen Handelns zu wählen, die bezogen auf den Zweck, der erreicht werden soll, den geringstmöglichen Eingriff in die Integrität des betroffenen Bürgers darstellt.

Meine Stellungnahme hat eine bundesweite, intensive Diskussion über den Sperrvermerk ausgelöst und ist auf große Resonanz in der Medienöffentlichkeit gestoßen. Die Diskussion hatte zur Folge, daß der Hessische Minister des Innern wie auch Innenminister anderer Länder angeordnet haben, Sperrvermerke im Bundespersonalausweis in Zukunft nicht mehr anzubringen.

Die intensive Diskussion hat auch besondere Aufmerksamkeit auf den Entwurf der Bundesregierung über ein Gesetz zur Änderung des Gesetzes über Personalausweise vom 25. Mai 1979, Drucks. 266/79 gelenkt. Dieser neue Entwurf beruht auf einem Beschluß der Innenminister der Länder vom 22. Juni 1978, in dem der Bundesminister des Innern gebeten worden war, die Einführung eines Systems neuer Personalausweise vorzubereiten, die fälschungssicher und maschinell lesbar sein sollten.

Nach der amtlichen Begründung des Entwurfs stellte sich der Bundesregierung zunächst „die Einführung des neuen Personalausweissystems in erster Linie als eine Änderung der gegenwärtig verwendeten Ausweismuster“ dar. Die wesentlich materiellen Änderungen des Gesetzes über Personalausweise ergaben sich daher aus der Sicht der Bundesregierung nur insoweit, als sie durch die technische Ausgestaltung des neuen Ausweissystems veranlaßt und zum Zweck des angestrebten Sicherheitsgewinns unumgänglich waren.

Im Rahmen meiner Beratungskompetenz habe ich bereits im Schreiben vom 12. Juni dem Hessischen Minister des Innern, dem

Bundesminister des Innern und dem Vorsitzenden des Innenausschusses des Deutschen Bundestages sowie auch den Datenschutzbeauftragten des Bundes und der Länder einen Änderungsvorschlag aus der Sicht des Datenschutzes unterbreitet, der im wesentlichen von zwei Grundsätzen ausging:

Daher ist im Gesetz positiv und erschöpfend festzulegen, welche Angaben im Personalausweis vom Gesetzgeber zugelassen werden. Diese Entscheidung darf nicht dem Verwaltungsverfahren überlassen werden.

Das Gesetz muß ferner sicherstellen, daß nicht eine zentral geführte Personendatei – etwa bei der Stelle, welche die Ausweise herstellt – entsteht. Das Bundesverfassungsgericht hat in seinem Beschluß vom 16. Juli 1969 zum Mikrozensus (BVerfGE 27, 1 ff.) festgestellt, daß es mit der Menschenwürde nicht vereinbar wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren, und zu katalogisieren, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.

Der Rechtsausschuß des Deutschen Bundestages hat bereits in seiner Stellungnahme zum Entwurf des Bundesdatenschutzgesetzes zum Ausdruck gebracht, daß die Entwicklung, Einführung und Verwendung von Nummerierungssystemen, die einheitliche Nummerierung der Bevölkerung im Geltungsbereich dieses Gesetzes ermöglichen (Personenkennzeichen) unzulässig ist.

Dieser Grundsatz gilt für alle bereichsspezifischen Regelungen staatlicher Informationsverarbeitung und trifft in besonderer Weise auf das Personalausweisgesetz und das beabsichtigte Verwaltungsverfahren zu. Es muß daher durch Gesetz ausgeschlossen werden, daß im Zuge eines derartigen Verwaltungsverfahrens zentrale Personendateien im Zusammenhang mit der Herstellung und Ausgabe der Personalausweise entstehen.

Die erforderlichen gesetzlichen Regelungen sollen dazu beitragen, das Informationsverhalten des Staates voraussehbar zu machen und Besorgnisse der Bürger vor staatlicher Informationstechnologie abzubauen.

1. Die für den Ausweis in Betracht kommenden Angaben sind im Gesetz abschließend festgehalten.
2. Die vorgesehene zentrale Herstellung der Bundespersonalausweise darf nicht dazu

benutzt werden, ein zentrales Register der Ausweisinhaber zu erstellen.

Die Landesregierung hat daraufhin in enger Zusammenarbeit mit mir einen Antrag zur 476. Sitzung des Bundesrates am 6. Juli 1979 vorbereitet, in der die Bundesregierung gebeten wird, „im weiteren Verlauf des Gesetzgebungsverfahrens mit Rücksicht auf den grundsätzlich notwendigen Schutz der Persönlichkeitssphäre ergänzende gesetzliche Regelungen in bezug auf das Muster der Ausweise vorzusehen, die

- die personenbezogenen Angaben auf das zur Feststellung der Personenidentität unbedingt erforderliche Maß beschränken und abschließend aufzuzählen
- und sicherstellen, daß aufgrund dieses Gesetzes keine zentrale Datei der Inhaber von Personalausweisen entsteht.

In der Begründung zu diesem Entschließungsantrag heißt es: Das Gesetz soll abschließend regeln, welche Angaben der Personalausweis enthalten darf.

In einem Gemeinwesen, dessen oberste Konstitutionsprinzipien die Menschenwürde und die Achtung vor der Persönlichkeit sind, muß der Bürger angesichts der technischen Entwicklung im Bereich der Informationsverarbeitung die Gewißheit haben, daß sein Personalausweis nicht zum Träger verschlüsselter Informationen werden kann. Das Informationsverhalten der Behörden und Ämter muß für den Bürger einsichtig und voraussehbar sein.

Obwohl dieser Entschließungsantrag von der Mehrheit der Mitglieder des Bundesrates abgelehnt wurde, haben seine Grundsätze maßgeblichen Einfluß auf die Vorlage genommen, die von den Koalitionsfraktionen angehörenden Berichterstattern des Innenausschusses des Deutschen Bundestages erarbeitet wurde, die sich dementsprechend durch eine wesentliche Verstärkung der datenschutzrechtlichen Sicherung auszeichnete. Diese Tatsache wird auch in der Beschlußempfehlung und dem Bericht des Innenausschusses (IV. Ausschuß) BT-Drucks. 8/3498 vom 12. Dezember 1979 Seite 8 besonders hervorgehoben. Mit der Verabschiedung des Bundespersonalausweisgesetzes nach der Beschlußempfehlung des Innenausschusses am 17. Januar 1980 sind die Vorschläge der Hessischen Landesregierung und des Hessischen Datenschutzbeauftragten im wesentlichen in die Tat umgesetzt worden. Allerdings ist die Verwendung der maschinenlesbaren Ausweis-

karte für Zwecke des Informationssystems der Sicherheitsbehörden nur unter der Voraussetzung annehmbar, daß zum einen ein datenschutzgerechtes Melderecht alsbald verabschiedet wird und zugleich bereichsspezifische Datenschutzvorschriften für die Sicherheitsbehörden erarbeitet werden. Diese Forderung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8. November 1979 noch einmal nachdrücklich bekräftigt. Der Deutsche Bundestag hat in einer Entschließung zum Bundespersonalausweisgesetz (vgl. Drucks. 8/3498 S. 3) sich diese Auffassung der Datenschutzbeauftragten zu eigen gemacht. Die Entschließung lautet: Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten.

Die Bundesregierung wird deshalb ersucht,

1. den Entwurf eines datenschutzrechtlichen Melderechtsrahmengesetzes einzubringen und
2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen.

2.7.2 Melderechtsrahmengesetz

Am 28. Dezember 1979 hat die Bundesregierung dem Bundesrat den Entwurf eines Melderechtsrahmengesetzes übersandt. Der vorliegende Gesetzentwurf hat zum großen Teil wesentliche Gesichtspunkte, die ich bereits am 20. November 1978 im Rahmen meiner Stellungnahme zum Entwurf eines Bundesmeldegesetzes bei der Anhörung am 20./21. November 1978 vorgetragen habe, berücksichtigt.

Dennoch wird die Effektivität des Melderechtsrahmengesetzes als bereichsspezifische Datenschutzregelung für die in ihrer Gesamtheit größte Sammlung personenbezogener Daten im öffentlichen Bereich in einem wesentlichen Punkt in Frage gestellt: Die Speicherung von Ausweisdaten im § 2 Abs. 1 Ziff. 15 stellt i. V. m. mit der vereinfachten Übermittlung an Sicherheits- und Strafverfolgungsbehörden im Sinne des § 18 Abs. 3 Melderechtsrahmengesetz und einem maschi-

nenlesbaren Personalausweisssystem ein räumlich verteiltes, aber logisch einheitliches Datenbanksystem für die Sicherheitsbehörden zur Verfügung.

Die gegenwärtige Fassung der §§ 18 Abs. 3 und 2 Abs. 1 Ziff. 15 des Entwurfs für ein Melderechtsrahmengesetz des Bundes steht im Widerspruch zu dem vom Gesetzgeber im gerade erst verabschiedeten Personalausweisgesetz getroffenen Entscheidungen. Der Gesetzgeber hat im Personalausweisgesetz, um einen wirksamen Datenschutz sicherzustellen, sowohl die Angaben, die in den Personalausweis aufgenommen werden dürfen, als auch die Verwendung dieser Angaben genau festgelegt. Deshalb wendet sich das Personalausweisgesetz ausdrücklich gegen jeden Versuch, die im Ausweis enthaltenen Angaben zu benutzen, um zentrale Dateien zu errichten. Genau dieses wird durch die Übermittlungsvorschriften des Entwurfs ermöglicht. Zwar sind die Personalausweisangaben dezentral bei den Meldebehörden gespeichert, unterliegen aber durch die Übermittlungsregelung dem direkten Zugriff der Sicherheits- und Strafverfolgungsbehörden. Auf diesem Weg kann die vom Gesetzgeber ausdrücklich untersagte zentrale Datei doch noch entstehen. Nicht umsonst hat der Deutsche Bundestag am 17. Januar 1980 zur Verabschiedung des Personalausweisgesetzes die auf S. 5 erwähnte Entschließung getroffen.

Der Entwurf ermöglicht es, über die Übermittlung, die Maschinenlesbarkeit des Personalausweises und die Informationssysteme der Sicherheitsbehörden ein Substrat für das Personenkennzeichen jedenfalls im Sicherheitsbereich zu schaffen. Auf die verfassungsrechtliche Bedenklichkeit aller Versuche, das Personenkennzeichen einzuführen, hatte der Rechtsausschuß des Deutschen Bundestages bereits im Zusammenhang mit der Verabschiedung des Bundesdatenschutzgesetzes hingewiesen. Diese Bedenken sind auch dort unvermindert zu berücksichtigen, wo, wie hier, eine Entwicklung begünstigt wird, die das abgelehnte Personenkennzeichen auf Umwegen einführt. Letztlich werden auch alle Bemühungen gefährdet, Amtshilfe in einer Weise zu regeln, die ohne die legitimen Aufgaben der Sicherheitsbehörden zu beeinträchtigen, den Schutz des Bürgers garantiert.

Man kann aber auch umgekehrt nicht leugnen, daß in dem vorgelegten Entwurf zum ersten Mal die Bereitschaft deutlich wird, die Verarbeitung personenbezogener Daten gezielt

einzu­schränken und im Interesse des Bürgers streng auch und gerade innerhalb der öffentlichen Verwaltung abzuschotten. Der Verwirklichung dieser Intention des Gesetzgebers dient auch ein Entschließungsantrag der Hessischen Landesregierung im Bundesrat, der im Zusammenwirken mit mir erarbeitet worden ist. Allerdings sind diese Intentionen durch die jüngsten Beratungen im Bundesrat in Gefahr geraten. Auf folgende Punkte ist vor allem hinzuweisen:

- Die im Entwurf enthaltene Aufgabende­finition verliert letztlich ihre Bedeutung, wenn den Meldebehörden beliebig weitere Aufgaben durch Landesrecht übertragen werden können. Unter Datenschutzge­sichtspunkten ist für die Tätigkeit der Meldebehörden die strikte Bindung an die Identitätsfeststellung der Einwohner ent­scheidend.
- Der Umfang der den Meldebehörden zur Verfügung stehenden Unterlagen wird in unzumutbarer Weise zu Lasten des Bür­gers erweitert. Für sie kommt es z. B. nicht darauf an zu wissen, warum jemand sein Wahlrecht nicht ausüben darf, ob er etwa geisteskrank ist. Der Datenschutz fordert, sich auf die Angaben zu beschrän­ken, die für die jeweilige Aufgabe not­wendig sind.
- Der Übermittlung sind praktisch keine Grenzen gesetzt. Die Kritik am Bundes­datenschutzgesetz war in erster Linie eine Kritik an seinen viel zu allgemein gehaltenen und für den Bürger nicht durch­schaubaren Formulierung. Deshalb be­stand von Anfang an Einigkeit darüber, daß es Aufgabe späterer Einzelregelungen sein müßte, die Übermittlungsvoraus­setzung zu präzisieren. Eine Abkehr von den konkreten Bestimmungen des Entwurfs (§ 18 Abs. 1) und einer Rückkehr zum Text des Bundesdatenschutzgesetzes kommt einem Verzicht auf die Chance einer bereichsspezifischen Datenschutzregelung gleich.

So sehr die vom Grundgesetz geforderte und in der Verfassung verankerte Gesetzgebungs­zuständigkeit der Länder respektiert werden muß, so wenig darf die Kompetenzregelung zum Anlaß genommen werden, um die Wirksamkeit des Datenschutzes im Meldebereich grundsätzlich in Frage zu stellen. Die Länder selbst haben den Bund immer wieder gedrängt, ein Melderechtsrahmengesetz vor­zulegen. Die Länder sind es aber auch gewe­

sen, die keinen Augenblick gezögert haben, ihre Datenschutzgesetz zu nutzen, um erkann­te Mängel des Bundesdatenschutzgesetzes zu korrigieren und den Datenschutz fortzuent­wickeln. Die schärfere Zweckbindung, der verschuldensunabhängige Schadensersatzan­spruch, die beabsichtigte Abschaffung der Gebührenpflicht bei der Erteilung von Aus­künften und die ausdrückliche Anerkennung eines Grundrechts auf Datenschutz sind Beispiele dafür. Diese Vorgeschichte ver­pflichtet. Sie zwingt dazu, alles zu unternehmen, um den Entwurf nicht zu verwässern, sondern um ihn im Gegenteil einzig und allein daraufhin zu überprüfen, wo noch mehr und noch besseres im Hinblick auf einen wirksamen Datenschutz getan werden kann. Die Bemühungen der Hessischen Landesregierung zeigen, daß sie sich dieser Verpflichtung im Interesse des Bürgers bewußt ist.

2.7.3 Änderung der Landeswahlordnung

Die Wahlordnungen des Bundes, der Länder sowie der Kommunen enthalten aus der Sicht des Datenschutzes unterschiedliche Regelun­gen zum Datenumfang des Wählerverzeich­nisses und der Wahlbenachrichtigung sowie der Übermittlung personenbezogener Da­ten.

Ich habe bereits im Oktober dieses Jahres einen Formulierungsvorschlag für eine Ände­rung der Wahlordnungen im Kreise der Datenschutzbeauftragten des Bundes und der Länder zur Diskussion gestellt, der von fol­genden Gesichtspunkten ausging:

1. Die an den verschiedenen Stellen in den einzelnen Wahlordnungen des Bundes und der Länder geregelten Zulässigkeits­voraussetzungen zur Übermittlung perso­nenbezogener Daten aus dem Wählerver­zeichnis, die überdies qualitativ verschie­dene Aussagen enthalten, sollten in einer Übermittlungsvorschrift zusammengefaßt werden. Dabei ist zu unterscheiden zwi­schen Übermittlungen im öffentlichen Bereich (jederzeit, nur an Stellen des Wahlgebietes, nur im Zusammenhang mit der Wahl) und Übermittlungen an Stellen außerhalb des öffentlichen Bereichs (nur innerhalb der Auslegungsfrist, an Perso­nen und Personenvereinigungen oder andere nicht-öffentliche Stellen, die an der Wahl beteiligt sind, Vorliegen eines berechtigten Interesses, schutzwürdige Belange des/der Betroffenen dürfen nicht berührt werden).

2. Abschriften aus dem Wählerverzeichnis sind aus Gründen des Datenschutzes – Umfang und Inhalt der Abschrift müssen nachprüfbar sein – nur durch die zuständige Behörde oder in deren Auftrag (Rechenzentrum) zulässig.
3. Maschinenlesbare Abschriften (Datenträger) dürfen nicht übermittelt werden, um die Gefahr unberechtigter Datenverarbeitung möglichst klein zu halten. Die Übermittlung ist zweckgebunden und somit an die entsprechende Regelung der Datenschutzgesetze angepaßt.
4. Das Institut des Sperrechts, wie es sich in § 16 a des Hessischen Meldegesetzes bewährt hat, sollte in die Wahlordnung aufgenommen werden. Es erleichtert die Definition der Übermittlungskriterien im nicht-öffentlichen Bereich.
5. Bei der Auslegung des Wählerverzeichnisses sollte dem Bürger die Möglichkeit geboten werden, daß auf seinen Antrag hin sein Geburtsdatum unkenntlich gemacht wird.
6. Die Wahlbenachrichtigung soll im Umfang der personenbezogenen Daten auf den Familiennamen, Vornamen und Wohnung des Wahlberechtigten beschränkt werden.

Wesentliche Teile dieses Vorschlags, den ich auch dem Hessischen Innenminister unterbreitet habe, sind inzwischen in die Bundeswahlordnung vom 8. November 1979 eingeflossen.

2.7.4 Grenzüberschreitender Datenverkehr

- a) Entwurf einer Konvention des Europarats
- b) Entwurf von Richtlinien der Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die beschränkten Wirkungsmöglichkeiten nationaler Regelungen zum Datenschutz für den internationalen bzw. grenzüberschreitenden Datenverkehr haben mich veranlaßt, auf die Dringlichkeit internationaler bzw. supranationaler Übereinkommen hinzuweisen. Derartige Übereinkommen können dort weiterhelfen, wo nationale bzw. föderale Regelungen versagen. Die Regelungsbedürftigkeit steht außer Frage. Im privaten wie im öffentlichen Bereich fließt ein reger Datenstrom über die Grenzen von Unternehmen zu Unternehmen, z. B. im multinationalen Konzern, von Finanzbehörden zu ausländischen Finanzbehörden

aufgrund bilateraler oder multilateraler Abkommen, aber auch innerhalb supranationaler Organisationen. Der Umfang der grenzüberschreitenden Datenproliferation nimmt mit der Entwicklung der Übertragungstechnologie exponentiell zu. Präsident Carter hat dem Kongress in seinem „Bericht zum Schutz der Privatsphäre“ vom 2. April 1979 mitgeteilt, das Außenministerium arbeite gegenwärtig mit anderen Ländern an Grundsätzen zum Schutz personenbezogener Daten beim grenzüberschreitenden Datenverkehr und zur Harmonisierung der nationalen Regelungen, um unnötige Unterbrechungen internationaler Kommunikationen vermeiden zu helfen. („To develop principles to protect personal data crossing international borders and to harmonise each country's rules to avoid needless disruptions of international communication“).

Inzwischen hat auch der auf Beschluß des Ministerkomitees des Europarats eingesetzte Expertenausschuß einen Entwurf eines „Übereinkommen(s) zum Schutz des einzelnen im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten“ (Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data) erarbeitet. Außerdem hat die vom Ausschuß für Forschung und Technologie der OECD eingesetzte Ad-hoc-Gruppe von Regierungsvertretern am 31. Mai 1979 einen Entwurf von „Richtlinien über den Schutz der Persönlichkeit und den grenzüberschreitenden Datenfluß“ [Draft Guidelines Governing the Projection of Privacy and Transborder Flows of Personal Data“ (Nr. DSTI/ICCP/79.40)] verabschiedet.

Von Beginn an habe ich auf den Einfluß derartiger Konventionen und Richtlinien auf Gesetzgebung in Bund und Ländern hingewiesen. Der Landesregierung habe ich Bedenken zu beiden Entwürfen mitgeteilt. Grundsätzlich habe ich die Initiative beider Organisationen außerordentlich begrüßt. Nicht nur deshalb, weil mit Hilfe beider eine dringend erforderliche Angleichung der nationalen Datenschutzbestrebungen erzielt und ein wichtiger Impuls für die Fortentwicklung der bereits bestehenden Bestimmungen vermittelt werden kann. Vielmehr hat sich gerade in jüngster Zeit immer wieder gezeigt, wie sehr es darauf ankommt, Vorschriften zum grenzüberschreitenden Datenaustausch vorzusehen. Allerdings hängt die Wirksamkeit derartiger Regelungen ganz entscheidend vom internationalen Konsens ab. Europarat und

OECD, nicht zuletzt aber auch das Europaparlament, können die Bedingungen für die Möglichkeit eines europäischen Konsenses in Fragen des Datenschutzes schaffen. Die Schwierigkeiten eines internationalen Übereinkommens für Datenschutz liegen auf der Hand: Weder ist die Struktur nationaler Regelungen vergleichbar, noch kann überhaupt von mehr oder weniger allgemein akzeptierten materiellrechtlichen Regelungen ausgegangen werden. Im Gegenteil, der Entwicklungsstand der beteiligten nationalen Rechtsordnungen ist höchst unterschiedlich. Einige Länder haben sehr detaillierte Regelungen, wie etwa die Bundesrepublik in Bund und Ländern, Frankreich, Österreich und Schweden; andere, wie Holland, Belgien, Spanien beginnen über Entwürfe zu diskutieren, während bei wieder anderen sich gerade in Regierungsgutachten ein Datenschutzbewußtsein zu manifestieren beginnt.

Internationale Übereinkommen, die sich nicht gezielt mit vorhandenen nationalen Regelungen auseinandersetzen, riskieren, wie die Erfahrung beweist, bloße Theorie zu bleiben. Der Entwurf des Europarats verzichtet angesichts dieser Konsequenz auf eine Bestimmung zum anwendbaren Recht (Art. 4), er verlangt vielmehr von den Vertragsparteien eine Konkretisierung der Grundprinzipien der Konvention in der innerstaatlichen Gesetzgebung. Mit anderen Worten, nicht eine kollisionsrechtliche Lösung des grenzüberschreitenden Datenaustausches wird angestrebt, sondern Minimalstandards für nationale Gesetzgebung. Solange konkrete Kollisionsregeln fehlen, die sich zum anwendbaren Recht äußern, ist eine abschließende Beurteilung der Konvention letztlich nicht möglich. Nicht nur, weil sich dann einmal mehr die Notwendigkeit einer bereichsspezifischen Regelung erweist, sondern auch und vor allem im Hinblick auf die daraus für die Rechte des Betroffenen folgenden Konsequenzen. Ich kann nur davor warnen, an diese Fragen mit den üblichen Kollisionsregeln heranzugehen. Der Datenschutz fügt sich nicht ohne weiteres in die hergebrachten Kategorien des internationalen Privatrechts ein. Ich habe daher die hessische Landesregierung gebeten, im Rahmen ihrer Möglichkeiten darauf einzuwirken, durch eine Kumulation von Anknüpfungspunkten die Chancen des betroffenen hessischen Bürgers, seine Rechte auch angesichts der zunehmenden Internationalisierung der Informationsverarbeitung durchzusetzen, möglichst zu erweitern.

Doch damit sind die Bedenken nicht erschöpft. In beiden Entwürfen ist vom grenzüberschreitenden Datenaustausch die Rede, ohne aber zwischen dem Informationsaustausch privater Unternehmen und der Übermittlung von Daten durch Behörden zu unterscheiden. Das Gefährdungspotential ist unzweifelhaft gleich, doch die Konsequenz eines beide Sachverhalte gleichermaßen regelnden Übereinkommens ist damit noch nicht angezeigt. Im Gegenteil, ein wirksamer Schutz des Bürgers setzt Regelungen voraus, die die Besonderheiten des jeweiligen Sachverhalts berücksichtigen. Kreditauskünfte über Grenzen hinweg sind eben anders zu beurteilen als die grenzüberschreitende Meldung genetischer Mißbildungen an supranationale Register; internationale Amtshilfe unterliegt anderen Kriterien als Informationsströme in multinationalen Unternehmen.

Zwar kann eingewandt werden, der Gesetzgeber selbst habe im BDSG schließlich beide Materien, Datenschutz im privaten und öffentlichen Bereich, in einem Gesetz geregelt. Der Preis ist freilich: Hoher Abstraktionsgrad und Generalklauseln, die letztlich die Wirksamkeit des Gesetzes zu unterlaufen im Stande sind. Die Effektivität von Rechtsnormen liegt in ihrer Sachnähe. Datenschutz setzt mit anderen Worten differenzierende Lösungen voraus. Mißverständliche Formulierungen tragen überdies dazu bei, den Schutz der persönlichen Integrität des Bürgers eher ins Gegenteil zu verkehren. Danach soll gem. Art. 12 Ziff. 1 des Konventionsentwurfs des Europarats eine Vertragspartei nicht berechtigt sein, „allein zum Zweck des Schutzes der Privatsphäre“, den grenzüberschreitenden Verkehr personenbezogener Daten in das oder aus dem Hoheitsgebiet einer anderen Vertragspartei von einer besonderen Genehmigung abhängig zu machen. Allein dieses Ziel reicht nach mittlerweile herrschender Interpretation des BDSG und der entsprechenden Landesgesetze vollauf, die Übermittlung personenbezogener Daten in ein anderes Land jedenfalls dann zu versagen, wenn dort keine entsprechenden Vorkehrungen zum Schutz des Bürgers vorhanden sind. Es ist daher von vornherein darauf zu achten, das Übereinkommen nicht mit Formulierungen zu befrachten, die unschwer als Instrument genutzt werden können, einen wirksamen Datenschutz zu unterlaufen.

In den OECD-Richtlinien (DSTI/ICCP/79.40 vom 31. Mai 1979) findet sich unter Ziff. 18 eine Formulierung, die datenschutzpolitisch

überaus bedenklich erscheint. Danach sollen die Vertragsparteien davon Abstand nehmen, „Gesetze, Grundsatzverfahren und Praktiken zu entwickeln, die über diejenigen hinausgehen, die für den angemessenen Schutz der Privatsphäre und der individuellen Freiheiten erforderlich sind und daher unvereinbar sind mit dem freien grenzüberschreitenden Verkehr personenbezogener Daten.“ Es ist nicht so recht einzusehen, was der Appell an die Mitgliedsländer der OECD bedeutet, sich beim Datenschutz zurückzuhalten, um nicht den freien grenzüberschreitenden Informationsaustausch zu gefährden, und zwar auch und gerade dann, wenn es um personenbezogene Daten geht. Sinn und Zweck der Leitlinien ist es ja gerade, den grenzüberschreitenden Datenaustausch im Interesse des Bürgers zu beschränken. Derartige Normprogramme können allzuleicht in einer Weise interpretiert werden, die auf eine Verpflichtung der Mitgliedsländer hinausläuft, sich zumindest bei weiteren Anstrengungen für einen besseren Datenschutz zurückzuhalten. Ebenso empfehle ich darauf hinzuweisen, daß Nr. 3 (b) gestrichen wird. Nr. 3 (b) besagt, daß diejenigen Daten der Anwendung der Leitlinien ausgenommen werden sollen, die offenkundig keine schutzwürdigen Belange von Bürgern verletzen können. Die Geschichte der Gesetzgebung in der Bundesrepublik Deutschland zeigt nur zu gut, daß es unmöglich ist, bestimmte Daten von vornherein als harmlos anzusehen. Die Diskussion um die „freien Daten“ ist dafür exemplarisch. Man sollte deshalb von solchen Feststellungen absehen und statt dessen mit dem in Nr. 3 (a) enthaltenen, richtigen Hinweis auf den Verwendungszusammenhang beschränken. All dies hat einen überaus realen Bezug für den zukünftigen Datenschutz hessischer Bürger im Kontext der internationalen Informationsverarbeitung, sei es im staatlichen, sei es im privaten Bereich.

Noch eine Bemerkung zur Organisation des internationalen Datenschutzes. Nach Art. 13 des Konventionsentwurfs des Europarats soll jede Vertragspartei eine hilfeleistende Behörde

benennen. Diese Behörde kann nach dem Entwurf auf Ersuchen einer von einer anderen Vertragspartei benannten Behörde

- a) Informationen über ihre Rechts- und Verwaltungspraxis im Bereich des Datenschutzes liefern;
- b) Sachinformationen über bestimmte Dateien mit personenbezogenen Daten liefern, die in ihrem Hoheitsgebiet verarbeitet werden; ausgenommen davon sind jedoch die in diesen Dateien enthaltenen personenbezogenen Daten;
- c) in Übereinstimmung mit den innerstaatlichen Rechtsvorschriften die in dem Antrag erbetenen Ermittlungen bezüglich einer Datei oder zur Datenverarbeitung verwendeter Einrichtungen, Geräte oder Methoden anstellen.

Überlegungen, das Bundesverwaltungsamt zur hilfeleistenden Behörde zu ernennen, halte ich aus sachlichen und verfassungsrechtlichen Gründen für problematisch. Schließlich kann es nicht darum gehen, neue Datenschutzbürokratien und neue Koordinierungsgremien zu schaffen, sondern vorhandenen Sachverstand und bestehende Institutionen so intensiv wie nur möglich zu nutzen. Ich habe daher angeregt, auch und gerade um der Verantwortung gegenüber den europäischen Vertragspartnern willen, den Bundesbeauftragten für den Datenschutz als hilfeleistende Behörde, die mit ausreichender Sachkompetenz ausgestattet ist, im Sinne des Art. 13 des Entwurfs des Datenschutz-Übereinkommens zu benennen. Ich gehe dabei allerdings davon aus, daß der Bundesbeauftragte für den Datenschutz im innerstaatlichen Verhältnis nur im Rahmen seiner Zuständigkeit tätig werden kann und im übrigen lediglich als Koordinationsinstanz und Postverteilungsstelle für die zuständigen Datenschutzbeauftragten und Aufsichtsbehörden der Länder fungiert. Dies ist bei der Notifizierung zu berücksichtigen.

Professor Dr. Simitis

3. DRITTER TEIL

3. Dritter Teil

Materialien

3.1 Kirchliche Datenschutzbestimmungen¹⁰⁾

I

1. Das Kirchengesetz der EKD über den Datenschutz – hier: EKD-Gesetz genannt – ist ein Grundsatz- oder Rahmengesetz. Es enthält nur Grundnormen des Datenschutzes und ermächtigt die Gliedkirchen für ihren Bereich und den Rat der EKD für deren Behörden und Stellen die zur Ergänzung und Durchführung dieses Kirchengesetzes erforderlichen Bestimmungen zu treffen:

§ 10

Ergänzende Bestimmungen

- (1) Die Gliedkirchen erlassen für ihren Bereich die zur Ergänzung und Durchführung dieses Kirchengesetzes erforderlichen Bestimmungen. Die Bestimmungen der Evangelischen Kirche in Deutschland erläßt der Rat durch Rechtsverordnungen.

Das EKD-Gesetz gilt in den Gliedkirchen, soweit sie es durch ein eigenes Kirchengesetz oder eine Kirchenverordnung übernehmen. Dies haben die evangelischen Kirchen in Hessen getan:

- Die evangelische Kirche von Kurhessen-Waldeck durch Verordnung vom 6. Januar 1978,
- die evangelische Kirche im Rheinland durch Kirchengesetz vom 12. Januar 1978,
- die evangelische Kirche in Hessen und Nassau durch Kirchengesetz vom 5. März 1978.

2. Darüber hinaus trifft das EKD-Gesetz in § 10 Abs. 2 folgende Regelung:

- (2) Soweit personenbezogene Daten von staatlichen oder kommunalen Stellen übermittelt werden, finden zum Schutz dieser Daten ergänzend die bundesrechtlichen Bestimmungen entsprechende Anwendung.

Zweck und Tragweite dieser Vorschrift sind problematisch.

Die Vorschrift könnte als eine Vorsorge-Klausel verstanden werden, die einerseits verhindern soll, daß die Übermittlung personenbezogener Daten aus dem staatlichen Bereich an kirchliche Stellen (§ 10 Abs. 2 BDSG – § 12 Abs. 2 HDStG) an dem Einwand der staatlichen Behörde scheitert, die Kirche habe keine ausreichende Datenschutzmaßnahmen getroffen, und andererseits die Gliedkirchen veranlassen soll, ergänzende Datenschutzregelungen zu treffen, um zu verhindern, daß staatliche Vorschriften in den kirchlichen Datenschutz unmittelbar eingreifen.

Die Vorschrift hat die Kritik der EK von Kurhessen-Waldeck hervorgerufen:

- Die Unterscheidung zwischen vom Staat gelieferten und von kirchlichen Stellen erhobenen Daten ließe sich praktisch kaum durchführen;
- in den Gemeindemitgliederverzeichnissen ließe sich nicht feststellen, woher die Daten stammen; wenn vom Staat, z. B. dem Einwohnermeldeamt, gelieferte Daten zur Person eines Kirchenmitgliedes durch Daten aus dem kirchlichen Bereich, z. B. über die kirchliche Trauung, ergänzt werden, entstehe ein einheitlicher Datensatz, der nur als Ganzes geschützt werden könne;
- es sei kein Grund ersichtlich, einen verschiedenen Datenschutz zu gewähren, je nachdem ob das Kirchenmitglied seine Daten selbst zur Verfügung stellt oder ob die Kirche sie vom Staat erhält;
(vgl. Begründung zur Verordnung über die Zustimmung der EKD von Kurhessen-Waldeck zum EKD-Gesetz Abschnitt 4).

Diese Kritik könnte für den Datenschutz im Bereich der Kirche berechtigt sein. Die Unterscheidung nach der Herkunft der Daten hat jedoch für die hier erörterte Frage, ob ausreichende Datenschutzmaßnahmen getroffen sind, nur Bedeutung, wenn sich ergibt, daß das kirchliche Recht einen qualitativ geringeren Datenschutz gewährleistet als das staatliche Recht. Insoweit ist die Vorschrift als eine Übergangsbestimmung aufzufassen, die solan-

¹⁰⁾ Zu Ziff. 2.6.2.

ge von Bedeutung ist, solange nicht die Gliedkirchen und der Rat der EKD die in § 10 Abs. 1 EKD-Gesetz für notwendig erachteten Bestimmungen zur Ergänzung und Durchführung des EKD-Gesetzes erlassen haben.

3. Nach dem Wortlaut des § 1 Abs. 1 des Kirchengesetzes scheinen **Gegenstand des Datenschutzes** (Schutzgut) die in den kirchlichen Dateien gespeicherten Daten zu sein:

„(1) Aufgabe des Datenschutzes im kirchlichen Bereich ist es, die in den Gemeindegliederverzeichnissen und anderen kirchlichen Dateien enthaltenen personenbezogenen Daten bei der Datenverarbeitung vor Mißbrauch zu schützen“.

Weder wird das Kirchenmitglied als Betroffener erwähnt, noch werden seine Belange als schutzwürdig bezeichnet. Gleichwohl ist Datenschutz nach dem Kirchengesetz nicht nur als Datensicherung zu verstehen. Vielmehr ergibt sich aus dem Gesamtzusammenhang des Gesetzes, wie aus den ergänzenden und ausführlichen Rechtsvorschriften der Gliedkirchen, daß Datenschutz auch im kirchlichen Bereich als personaler Schutz des Betroffenen und seiner Belange vor mißbräuchlicher Verwendung seiner Daten verstanden wird. Dies folgt insbesondere aus den Vorschriften des EKD-Gesetzes, welche die Rechtsstellung des Kirchenmitgliedes bestimmen:

- Das **Auskunftsrecht** des Kirchenmitgliedes, das in diesem Zusammenhang als Betroffener im Sinne der staatlichen Datenschutzgesetze bezeichnet wird (§ 4);
- die **Vorrangigkeit** der besonderen Bestimmungen über den Schutz des **Beicht- und Seelsorgegeheimnisses** sowie über die **Amtsverschwiegenheit** der Pfarrer und kirchlichen Mitarbeiter (§ 1 Abs. 2 – vergleichbar mit § 35 HDSG und § 45 S. 1 Nr. 1 BDSG);
- das **Privileg der Pfarrer** und kirchlichen Mitarbeiter, in Wahrnehmung ihres Seelsorgeauftrages über ihren Dienst an Kirchenmitglieder eigene Aufzeichnungen zu führen und zu verwenden (§ 1 Abs. 3 – vergleichbar dem Presse- und Rundfunkprivileg nach § 1 Abs. 3 BDSG und § 3 Abs. 3 HDSG).

4. Ein grundsätzlicher Unterschied zwischen dem kirchlichen und dem staatlichen Datenschutz könnte sich aus der **Verschiedenartigkeit der Methoden**, mit welcher Datenschutz

verwirklicht werden soll, ergeben. Während die staatlichen Datenschutzgesetze bei der Datenverarbeitung und deren Reglementierung nach dem Modell des Verbots mit Erlaubnisvorbehalt ansetzen, d. h. die Datenverarbeitung überhaupt nur zulassen, wenn gesetzlich festgelegte Voraussetzungen erfüllt sind, verbietet das Kirchengesetz, die geschützten personenbezogenen Daten der Kirchenmitglieder zu anderen Zwecken als zur Erfüllung der kirchlichen Aufgaben zu verarbeiten und zu nutzen; es stellt also nicht auf den äußeren Vorgang der Sammlung von Daten, das Datenspeichern, sondern auf die Verwendung der Daten ab, ohne deren Beschaffung (Erfassung) einer Regelung zu unterwerfen:

§ 2

Datennutzung im kirchlichen Bereich

- (1) Kirchliche Behörden, sonstige kirchliche Dienststellen sowie kirchliche Werke und Einrichtungen der Evangelischen Kirche in Deutschland und ihrer Gliedkirchen dürfen geschützte personenbezogene Daten nur für die Erfüllung ihrer Aufgaben verarbeiten und nutzen. Den Pfarrern und kirchlichen Mitarbeitern in den in Satz 1 bezeichneten kirchlichen Stellen ist es untersagt, diese Daten zu einem anderen Zweck zu nutzen.
- (2) Die in Abs. 1 bezeichneten kirchlichen Stellen, Pfarrer und kirchlichen Mitarbeiter sind zur Einhaltung der Bestimmungen verpflichtet, die zum Schutz der personenbezogenen Daten vor Mißbrauch erlassen sind.

Geschützte personenbezogene Daten im Sinne des Gesetzes sind die in § 1 genannten „in den Gemeindegliederverzeichnissen und anderen kirchlichen Dateien enthaltenen personenbezogenen Daten“ (vgl. oben 3.).

Der methodische Unterschied folgt aus der Verschiedenartigkeit sowohl der staatlichen und der kirchlichen Aufgaben, als auch der Rechtsgrundlagen, auf denen sie beruhen. Dies kommt insbesondere in der strengen Bindung der staatlichen Behörden an den verfassungsrechtlichen Grundsatz der Gesetzmäßigkeit der Verwaltung zum Ausdruck, der im kirchlichen Bereich für die Bestimmung der kirchlichen Aufgaben und deren Erfüllung durch die kirchlichen Behörden und Stellen keine Entsprechung hat.

Vielmehr stellt sich die Kirche ihre Aufgaben aus ihrem Selbstverständnis heraus und unter-

liegt daher innerhalb ihres Bereiches nur selbst bestimmten Schranken. Hierzu sagen die Grundbestimmungen und die Aufgabenbeschreibung in der Grundordnung der EKD vom 13. Juli 1948 (ABl. der EKD 1948, Nr. 80) folgendes aus:

Artikel 3

(1) Die Evangelische Kirche in Deutschland ist um ihres Auftrages willen unabhängig in der Aufstellung ihrer Grundsätze, in der Ordnung und Verwaltung ihrer Angelegenheiten und in der Verleihung und Aberkennung ihrer Ämter.

(2) Die Regelung ihres Verhältnisses zum Staat bleibt einem Übereinkommen vorbehalten.

Artikel 15

(1) Die Evangelische Kirche in Deutschland und die Gliedkirchen sind gerufen, Christi Liebe in Wort und Tat zu verkünden. Diese Liebe verpflichtet alle Glieder der Kirche zum Dienst und gewinnt in besonderer Weise Gestalt im Diakonat der Kirche; demgemäß sind die diakonisch-missionarischen Werke Wesens- und Lebensäußerung der Kirche.

(2) Die Evangelische Kirche in Deutschland fördert die in ihrem Gesamtbereich arbeitenden Werke der Inneren Mission, ungeachtet deren Rechtsform. Ihre Verbindung mit der Kirche und den Gemeinden sowie die freie Gestaltung ihrer Arbeit werden in Vereinbarungen und entsprechenden Richtlinien gesichert.

(3) Das Hilfswerk der Evangelischen Kirche in Deutschland wird von der Evangelischen Kirche in Deutschland, den Gliedkirchen und ihren Gemeinden getragen. Es dient dem kirchlichen Wiederaufbau sowie der Linderung und Behebung der Notstände der Zeit. Die Ordnung des Hilfswerkes bedarf eines Gesetzes der Evangelischen Kirche in Deutschland¹¹⁾.

Artikel 16

(1) Die Evangelische Kirche in Deutschland und die Gliedkirchen wissen, daß die Kirche Christi das Evangelium an die ganze Welt zu bezeugen hat. Im Gehorsam gegen den Sendungsauftrag ihres Herrn treiben

sie das Werk der Äußeren Mission. Die Evangelische Kirche in Deutschland fördert die Arbeit der Äußeren Mission in Zusammenarbeit mit der von den Missionsgesellschaften bestellten Vertretung. Sie kann für diese Zusammenarbeit Grundsätze aufstellen.

(2) Ebenso weiß sich die Evangelische Kirche in Deutschland zum Dienst an der evangelischen Diaspora berufen. Sie fördert die zur Erfüllung dieses Dienstes bestehenden Einrichtungen und die anderen kirchlichen Werke, soweit sie im Gesamtbereich der Evangelischen Kirche in Deutschland ihren Dienst tun. Sie kann ihnen unter Wahrung ihrer sachlich erforderten Selbständigkeit für ihre Arbeit und ihre Ordnung Richtlinien geben.

Ungeachtet dieses Unterschiedes stimmt das kirchliche Datenschutzrecht in der Zielsetzung in der Mißbrauchsverhütung zum Schutz des Betroffenen mit dem staatlichen Datenschutzrecht überein.

5. Übereinstimmung mit dem staatlichen Datenschutzrecht besteht ferner in den weiteren Vorschriften des Kirchengesetzes:

– Dateienregister:

Die EKD und die Gliedkirchen haben jeweils für ihren Bereich eine Übersicht zu führen über:

1. die Art der gespeicherten personenbezogenen Daten,
2. die Aufgabe, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist und
3. deren regelmäßige Empfänger (§ 3 Abs. 2).

– Auskunft:

Den Betroffenen ist auf ihren Antrag Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. Diese Auskunftspflicht unterliegt den gleichen Einschränkungen wie in § 18 Abs. 3 Nr. 1 – wobei auf die Erfüllung des der speichernden Stelle obliegenden Kirchenauftrages und dessen Gefährdung abgestellt ist – und Nr. 2 HDSG.

Die Ausnahmen in den Nrn. 2 und 4 des § 18 Abs. 3 HDSG fehlen im Kirchengesetz; die Sachverhalte haben im kirchlichen Bereich keine Entsprechung. Anders als in § 18 Abs. 4 HDSG ist die Auskunft

¹¹⁾ Kirchengesetz über den Zusammenschluß von Innerer Mission und Hilfswerk der EKD vom 8. März 1957 (ABl. EKD 1957, Nr. 70).

gebührenfrei. Auch die – bisher allein vorliegende – Durchführungsverordnung der EK im Rheinland beläßt es bei der Gebührenfreiheit.

– **Berichtigung:**

Die Regelung in § 5 stimmt mit § 19 Abs. 1 HDSG wörtlich überein. Die Sperrung und Löschung von Daten ist der Regelung durch die Gliedkirchen überlassen (siehe II 6).

– **Beauftragter für den Datenschutz:**

Nach § 6 bestellen die EKD und die Gliedkirchen jeweils für ihren Bereich einen Datenschutzbeauftragten. Es darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt (§ 6 Abs. 2).

Der Beauftragte für den Datenschutz bei der EKD untersteht der Rechtsaufsicht des Rates der EKD und der Dienstaufsicht des Präsidenten der Kirchenkanzlei. Die Rechtsstellung der Beauftragten für den Datenschutz in den Gliedkirchen regeln diese (§ 6 Abs. 6).

Die Beauftragten für den Datenschutz sind in Ausübung ihres Amtes an Weisungen nicht gebunden und nur dem kirchlichen Recht unterworfen (§ 6 Abs. 4). Ihre Aufgaben im kirchlichen Bereich entsprechen denen der staatlichen Datenschutzbeauftragten.

– **Anrufungsrecht:**

Wer darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten durch eine kirchliche Stelle in seinen Rechten verletzt worden ist, kann sich an den Beauftragten für den Datenschutz wenden, wenn die zuständige Stelle nicht abhilft (§ 8).

Demgegenüber ist das Anrufungsrecht im staatlichen Bereich nicht an die Voraussetzungen gebunden, daß die speichernde Stelle vergeblich um Abhilfe ersucht worden ist. Dieser Unterschied erklärt sich aus der Verschiedenartigkeit des Verhältnisses des Betroffenen zum Staat und zu seiner Kirche.

II¹²⁾

1. Aufgrund von § 10 Abs. 1 des übernommenen EKD-Gesetzes hat die EK im Rheinland in der Durchführungsverordnung vom 11. Mai 1978 die Rahmenregelung des EKD-Gesetzes ausgefüllt und sich dabei weitgehend an das Bundesdatenschutzgesetz angelehnt.

2. Im 1. Abschnitt „Gegenstand des Datenschutzes“ werden – ungeachtet des methodischen Unterschiedes, der oben (I 4) erläutert ist – die Begriffe personenbezogene Daten, Datei, Datenverarbeitung, speichern, verändern, übermitteln und löschen in gleicher Weise definiert wie in § 1 Abs. 1 und § 2 BDSG. Nicht definiert werden die Begriffe der speichernden Stelle und des Dritten, obwohl sie in den weiteren Vorschriften der Verordnung benutzt werden.

In die Begriffsbestimmung der Datei wird zugleich der Ausschluß von Akten und Akten-sammlungen aus dem Geltungsbereich der Verordnung entsprechend § 1 Abs. 2 S. 2 BDSG bestimmt.

Für die sog. internen Daten (§ 2 Abs. 2 S. 2 BDSG), deren Sammlung als „Handkartei“ bezeichnet wird, ist in Anlehnung an § 1 Abs. 2 HDSG bestimmt, daß sie nach Maßgabe der für personenbezogene Daten zu treffenden technischen und organisatorischen Maßnahmen „unter Verschuß“ zu halten sind (3.1).

3. Abweichend von der Methode des EKD-Gesetzes (§ 2), das von der Datennutzung ausgeht, wird im Abschnitt „Datenschutzregelungen für bestimmte Arbeitsbereiche“ folgendes bestimmt:

3.1 **Datenspeicherung (2.2)**

„Das Speichern und das Verändern personenbezogener Daten ist zulässig, wenn es zur Erfüllung des der speichernden Stelle obliegenden kirchlichen Auftrags erforderlich ist. Werden Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.“

Mit dieser Vorschrift werden für das Speichern und das Verändern personenbezogener Daten Zulässigkeitsvoraussetzungen aufgestellt, die dem Wortlaut nach denjenigen in § 9 Abs. 1 BDSG und § 11 HDSG ähneln. Sie werden jedoch dadurch relativiert, daß – richtiger-

¹²⁾ Zu Ziff. 2.6.3.

weise – auf die „Erforderlichkeit zur Erfüllung des der speichernden Stelle obliegenden **kirchlichen Auftrags**“ abgestellt wird. Die kirchlichen Aufträge, die der speichernden Stelle obliegen, leiten sich aus den Aufgaben ab, die sich die Kirche aus ihrem Selbstverständnis heraus für ihren umfassenden Dienst am Menschen stellt und die ihrem Wesen nach keiner Legalisierung durch förmliches Gesetz bedürfen. Der rechtliche Gehalt der Vorschrift deckt sich daher mit demjenigen des § 2 EKD-Gesetzes, wonach geschützte personenbezogene Daten nur für die Erfüllung der kirchlichen Aufgaben verarbeitet und genutzt werden dürfen (vgl. oben I 4).

Nach Satz 2 der Vorschrift ist das betroffene Kirchenmitglied auf die kirchliche Rechtsvorschrift, kraft welcher bei ihm Daten erhoben werden, oder auf die Freiwilligkeit seiner Angaben hinzuweisen. Diese Bestimmung ist eine – unreflektierte – Übernahme des § 9 Abs. 2 BDSG, der von einer ganz anderen Grundlage ausgeht: Er führt nämlich den in § 3 BDSG konkretisierten Grundsatz der Gesetzmäßigkeit der Verwaltung fort, wonach die Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine gesetzliche Vorschrift oder wenn der Betroffene durch seine Einwilligung sie erlaubt. Dieser Grundsatz ist dem kirchlichen Datenschutzrecht fremd. Die Aktivitäten der Kirche haben ihre Grundlage in den selbst gestellten Aufgaben und in den daraus abgeleiteten Kompetenzen der verfaßten Kirche gegenüber ihren Mitgliedern. Sie bedürfen keiner Legitimation durch förmliches Gesetz.

Diese Zweifel an dem materiellen Gehalt der Vorschrift geben jedoch keinen Anlaß, den kirchlichen Datenschutz abzuwerten. Demzufolge ist es auch unwichtig, daß der die Rechtsstellung des Betroffenen verbessernde Zusatz im § 11 Abs. 2 S. 2 HDSG:

„Dem Betroffenen dürfen aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen.“

nicht in Abschnitt 2.2 der Kirchenverordnung übernommen worden ist.

3.2 Datenverarbeitung im Auftrag (2.1)

Die Auftragsverarbeitung ist im wesentlichen in gleicher Weise geregelt wie in § 4 HDSG:

So ist die Datenverarbeitung durch Personen oder Stellen außerhalb der verfaßten Kirche nur im Rahmen der Weisungen der kirchlichen Stelle, die den Auftrag erteilt hat, zulässig.

Sofern die kirchlichen Datenschutzbestimmungen auf den Auftragnehmer keine Anwendung finden, hat der Auftraggeber sicherzustellen, daß die Bestimmungen der Durchführungsverordnung beachtet und der Auftragnehmer sich der Kontrolle des kirchlichen Datenschutzbeauftragten unterwirft.

Diese kirchenrechtliche Vorschrift läßt die staatliche Datenschutzregelung unberührt; das bedeutet im Geltungsbereich des HDSG folgendes: Ist der Auftragnehmer eine Behörde oder öffentliche Stelle (vgl. § 4 Abs. 1 S. 2 des Hessischen Datenverarbeitungsgesetzes vom 16. Dezember 1969), so gelten an Stelle der „Einzelregelungen für den Datenschutz“ (Zweiter Teil des HDSG) Vorschriften des BDSG für Dienstleistungsunternehmen (§ 31 Abs. 1 Nr. 3, II 37 ff.) mit der Folge, daß die staatliche Aufsichtsbehörde, in Hessen der Regierungspräsident, die Kontrolle über die Einhaltung der Datenschutzvorschriften ausübt (§ 40 BDSG). Diese Kontrolle erstreckt sich auch auf die Einhaltung der Weisungen der Auftraggeber (§ 37 BDSG), obwohl deren Einhaltung zugleich vom kirchlichen Datenschutzbeauftragten überwacht wird, wozu sich der Auftragnehmer verpflichtet haben muß. Daneben bleiben gemäß § 4 Abs. 2 HDSG die Rechte und Pflichten des Hessischen Datenschutzbeauftragten (§ 23 HDSG) bestehen. Er überwacht die Einhaltung der Vorschriften des Ersten Teils des HDSG, namentlich die Durchführung der Vorschriften nach §§ 5 und 6, die Wahrung des Datengeheimnisses nach § 9 und die technischen und organisatorischen Maßnahmen nach § 10 a. a. O.

Eine Beauftragung von Personen oder Stellen außerhalb der verfaßten Kirche bedarf der Genehmigung des Landeskirchenamtes. Für die Beauftragung des rheinischen Rechenzentrums für Kirche und Diakonie (RKD) gilt die Genehmigung als allgemein erteilt.

Kirchliche Stellen im Sinne dieser Vorschrift sind die in § 2 Abs. 1 EKD-Gesetz genannten, nämlich kirchliche Behörden, sonstige kirchliche Dienststellen sowie kirchliche Werke und Einrichtungen der Evangelischen Kirche in Deutschland und ihrer Gliedkirchen.

3.3 Übermittlung durch kirchliche Stellen an Dritte (2.3)

Die Regelung der Datenübermittlung durch kirchliche Stellen entspricht trotz abweichender Systematik den Vorschriften in § 12 Abs. 1 S. 1 und § 16 Abs. 1 S. 1 HDSG:

Die Übermittlung ist immer nur dann zulässig, wenn sie zur Erfüllung des kirchlichen Auf-

trages erforderlich ist, der der übermittelnden Stelle oder dem Empfänger obliegt:

a) Unter dieser Voraussetzung ist die Übermittlung personenbezogener Daten an **Kirchenbehörden und sonstige kirchliche Stellen** der verfaßten Kirche gemäß § 2 Abs. 1 des EKD-Gesetzes zulässig (2.3.1).

b) Davon unterschieden wird die Übermittlung personenbezogener Daten an **kirchliche Werke, Verbände und Einrichtungen**, die nicht unter § 2 Abs. 1 des EKD-Gesetzes fallen, insbesondere solche in **privatrechtlicher Trägerschaft**. In diesen Fällen ist weitere Voraussetzung, daß sichergestellt ist, daß bei dem Empfänger Datenschutzmaßnahmen entsprechend diesem Kirchengesetz getroffen worden sind (2.3.2).

Welche kirchlichen Werke, Verbände und Einrichtungen nicht von § 2 Abs. 1 EKD-Gesetz erfaßt werden, ist ein besonderes Problem im Hinblick auf die BVerfGE 46, 73ff. (Stiftung Wilhelm-Anton-Hospital in Goch) und weil § 2 Abs. 1 EKD-Gesetz nicht zwischen den kirchlichen Werken und Einrichtungen mit öffentlich-rechtlichem und solchen mit privat-rechtlichem Status unterscheidet (s. I 4.).

c) Zu den Einrichtungen im Sinne dieser Vorschrift gehören die kirchlichen Publikationsorgane „Der Weg“, „Sonntagsgruß“, „Glaube und Heimat“, „Deutsches Allgemeines Sonntagsblatt“ und „Evangelische Kommentare“.

Während § 1 Abs. 3 BDSG der Datenverarbeitung der Presse „ausschließlich zu eigenen publizistischen Zwecken“ von der Geltung des Gesetzes – zur Wahrung der in Art. 5 GG verbürgten Pressefreiheit – ausnimmt, stellt das Kirchenrecht darauf ab, ob die kirchlichen Presseorgane mit ihren Veröffentlichungen kirchliche Aufgaben oder kirchliche Aufträge erfüllen. Insoweit sind sie als kirchliche Werke und Einrichtungen dem kirchlichen Datenschutzrecht unterworfen.

In einer besonderen Verwaltungsanweisung „Datenschutz – Übermittlung von Daten der Gemeindeglieder –“ vom 12. September 1978 (KABl. S. 187 = ABl. der EKD vom 15. Januar 1979 S. 76) ordnet das Landeskirchenamt folgendes an: Die Übermittlung von personenbezogenen Daten an die genannten Publikationsorgane ist nach § 2 Abs. 1 EKD-Ge-

setz i. V. m. Nr. 2.3.2 dieser Durchführungsverordnung zulässig, weil die Übermittlung zur Erfüllung der kirchlichen Aufgaben der kirchlichen Körperschaften und des kirchlichen Auftrages der genannten Publikationsorgane erforderlich ist.

Darüber hinaus, d. h. für Betätigungen, welche außerhalb des kirchlichen Auftrags oder der kirchlichen Aufgabe liegenden Zwecken dienen, unterliegen sie den Regeln des Dritten Abschnitts des BDSG oder sind von dessen Geltung nach § 1 Abs. 3 – „für eigene publizistische Zwecke“ – ausgenommen.

Übermittelt werden dürfen jeweils nur die personenbezogenen Daten, welche für den jeweiligen Zweck erforderlich sind: nämlich für die Werbung und den Bezug der Zeitungen und Zeitschriften nur der Name und die Anschrift; für die Veröffentlichung von Taufen, Konfirmationen, Trauungen, Jubiläen, Geburtstagen der Name, die Daten der Amtshandlung sowie Ort bzw. Ortsteil.

Darüber hinaus wird die Veröffentlichung von Amtshandlungen, Jubiläen und Geburtstagen in den vorgenannten Publikationsorganen sowie in Gemeindebriefen und bei Kanzelabkündigungen nach § 2 Abs. 1 des EKD-Gesetzes i. V. m. Nr. 2.3.5 dieser Durchführungsverordnung für zulässig erklärt, weil die Veröffentlichung zur Erfüllung des kirchlichen Auftrages der übermittelnden Stelle erforderlich ist. Dabei dürfen wiederum nur der Name, die Daten der Amtshandlung sowie der Ort bzw. Ortsteil veröffentlicht werden.

Schließlich wird für unzulässig erklärt, Daten an Banken, Sparkassen und Geschäfte nach Nr. 2.3.5 dieser Durchführungsverordnung zu übermitteln weil die übermittelten Daten nicht der Erfüllung kirchlicher Aufgaben, sondern rein kommerziellen Zwecken dienen. Es könnte nicht ausgeschlossen werden, daß in diesen Fällen schutzwürdige Belange beeinträchtigt werden.

Soweit es sich um die Übermittlung an die kirchlichen Publikationsorgane nach 2.3.2 der Durchführungsverordnung handelt, fällt auf, daß in der Verwaltungsanweisung die nach 2.3.2 der Verordnung geforderte Sicherstellung ausreichender Datenschutzmaßnahmen beim Empfänger nicht erwähnt werden. Im übrigen kommt es hierbei in Abweichung von der entsprechenden Regelung nach dem HDSG

in keinem Falle auf die Einwilligung des Betroffenen an, weil die Veröffentlichung in den kirchlichen Publikationsorganen als Bestandteil der kirchlichen Aufgaben und des kirchlichen Auftrages betrachtet wird.

- d) Die Übermittlung an Stellen anderer **öffentlich-rechtlicher Religionsgesellschaften** ist unter den gleichen Voraussetzungen zulässig wie die an kirchliche Werke, Verbände und Einrichtungen im Sinne des § 2 Abs. 1 des EKD-Gesetzes (2.3.3).
- e) Die Übermittlung personenbezogener Daten an **Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden und Gemeindeverbände** und der sonstigen der Aufsicht des Bundes oder eines Landes unterstehenden juristischen Person des öffentlichen Rechts und für deren Vereinigungen ist zulässig, wenn sie zur Erfüllung des Auftrages, welcher der übermittelnden Stelle oder welcher dem Empfänger obliegt, erforderlich ist (2.3.4). Soweit gleicht die Regelung dem § 12 Abs. 1 S. 1 HDSG. Darüber hinaus hat die speichernde kirchliche Stelle noch zu prüfen, ob die Übermittlung nach staatlichem oder kirchlichem Recht erlaubt ist (vgl. E 2.4.5)
- f) Die Übermittlung personenbezogener Daten an **Personen und andere Stellen**, das soll heißen an Personen und Stellen, die nicht zum kirchlichen Bereich gehören, ist wie in § 16 Abs. 1 HDSG geregelt, wobei wiederum die „Erfüllung des kirchlichen Auftrags“ an die Stelle der „rechtmäßigen Erfüllung der zuständigen Aufgabe“ tritt (2.3.5).
- g) Eine besondere Regelung der Übermittlung solcher personenbezogenen Daten, die im kirchlichen Bereich einem Berufs- oder besonderem Amtsgeheimnis im Sinne des § 12 Abs. 1 S. 2 des § 16 Abs. 1 S. 2 HDSG unterliegen, fehlt in der Durchführungsverordnung. Sie ist auch nicht erforderlich, weil die besonderen Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses sowie über die Amtsverschwiegenheit der Pfarrer und kirchlichen Mitglieder nach § 1 des EKD-Gesetzes den Vorrang haben.

3.4 **Datenverarbeitung im Rahmen der Personalsachbearbeitung (2.4)**

Für die Datenverarbeitung, die frühere, bestehende oder zukünftige dienst- oder arbeits-

rechtliche Rechtsverhältnisse betrifft, ordnet die Durchführungsverordnung die Geltung der §§ 23 bis 27 BDSG an.

3.5 **Verpflichtung der Mitarbeiter (2.5)**

Die mit der Führung der Gemeindemitgliederverzeichnisse (§ 14 Kirchenmitgliedschaftsgesetz) oder sonst mit der Datenverarbeitung personenbezogener Daten beauftragten Mitarbeiter sind entsprechend der Regelung in § 9 Abs. 2 HDSG bei der Aufnahme ihrer Tätigkeit besonders über den Datenschutz zu belehren und auf seine Einhaltung schriftlich zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

4. **Durchführung des Datenschutzes (3.)**

Unter diesem Abschnitt werden Vorschriften über die technischen und organisatorischen Maßnahmen, über die kirchliche Aufsicht und über das Register, das nach § 3 Abs. 3 des EKD-Gesetzes geführt werden muß, getroffen, diese Vorschriften entsprechen § 10 HDSG bzw. § 15 BDSG.

5. **Auskunft an Betroffene (4.)**

Die Verordnung nimmt Bezug auf das in § 4 des EKD-Gesetzes geregelte Auskunftsrecht des Betroffenen und bestimmt die zur Auskunftserteilung verpflichteten Stellen. Zugleich wird das kirchliche Rechenzentrum mit der Erteilung der Auskünfte beauftragt, soweit es die Gemeindemitgliederdaten im Auftrag der kirchlichen Körperschaften speichert. Hier wird im Gegensatz zu der Regelung im staatlichen Bereich, die auf der Trennung der Verwaltungsaufgabe von dem technischen Vorgang der Verarbeitung von Daten im Rechenzentrum angelegt ist, dem kirchlichen Rechenzentrum die Erteilung der Auskunft als Verwaltungsaufgabe zugewiesen.

6. **Weitere Datenschutzmaßnahmen (5.)**

In Ausführung und in Ergänzung des § 5 des EKD-Gesetzes werden die Institute der Sperrung und der Löschung in Übereinstimmung mit § 19 Abs. 2 und § 3 HDSG geregelt. Anstelle des Kriteriums der rechtmäßigen Erfüllung der in der Zuständigkeit der amtlichen Stelle liegenden Aufgabe tritt wiederum der Bezug auf die Erfüllung des der kirchlichen Stelle obliegenden kirchlichen Auftrages.

7. **Datenschutzbeauftragter (6.)**

Der kirchliche Datenschutzbeauftragte wird von der Kirchenleitung für eine Amtszeit von vier Jahren berufen; die Wiederberufung ist zulässig; die Dienstaufsicht führt die Kirchenleitung. Berufung und Dienstsitz werden im kirchlichen Amtsblatt bekanntgegeben.

In Anlehnung an § 8 Abs. 3 BDSG wird ferner bestimmt (6.2), daß der kirchliche Datenschutzbeauftragte auch für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts zuständig ist, wenn sie personenbezogene Daten im Auftrag kirchlicher Stellen verarbeiten, sofern der

Evangelischen Kirche im Rheinland oder ihren öffentlich-rechtlichen Körperschaften die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht. Darauf ist die staatliche Aufsichtsbehörde (§§ 30, 40 BDSG) hinzuweisen; deren Befugnisse bleiben unberührt.

Darüber hinaus haben privatrechtlich geführte Einrichtungen (z. B. diakonische Werke, Rechenzentrum für Diakonie) unter den Voraussetzungen der §§ 28 und 38 BDSG einen betrieblichen Datenschutzbeauftragten, der der Leitung unmittelbar unterstellt ist, zu bestellen.

3.2 Vergleichende Übersicht

Bundesdatenschutzgesetz
– BDSG –

Anordnung über den kirchlichen Datenschutz
– K D O –

Erster Abschnitt**Allgemeine Vorschriften**

§ 1

Aufgabe und Gegenstand des Datenschutzes

(1) Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

(2) Dieses Gesetz schützt personenbezogene Daten, die

1. von Behörden oder sonstigen öffentlichen Stellen (§ 7),
2. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts für eigene Zwecke (§ 22),
3. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für fremde Zwecke (§ 31),

in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Für personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind und in nicht automatisierten Verfahren verarbeitet werden, gilt von den Vorschriften dieses Gesetzes nur § 6.

(3) Dieses Gesetz schützt personenbezogene Daten nicht, die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden; § 6 Abs. 1 bleibt unberührt.

§ 2

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person (Betroffener).

(2) Im Sinne dieses Gesetzes ist

1. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem

§ 1 Aufgabe und Gegenstand des Datenschutzes im kirchlichen Bereich

(1) Aufgabe des Datenschutzes im kirchlichen Bereich ist es, ...

(2) ...

die vom Bistum, von den Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbänden und von den ihrer Aufsicht unterstehenden kirchlichen Körperschaften, Stiftungen, Anstalten, Werken und Einrichtungen sowie im Auftrag dieser Stellen

(3) Soweit besondere kirchliche oder staatliche Rechtsvorschriften auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieser Anordnung vor.

(4) Unberührt von dieser Anordnung bleibt die Verpflichtung zur Verschwiegenheit über die in Ausübung priesterlicher oder seelsorglicher Tätigkeit erworbenen Kenntnisse über persönliche Angelegenheiten dritter Personen. Das gleiche gilt für die dienstliche Schweigepflicht.

§ 2 Begriffsbestimmungen

gleichlautend

Datenträger zum Zwecke ihrer weiteren Verwendung.

2. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden.
 3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten.
 4. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,
- ungeachtet der dabei angewendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist

1. speichernde Stelle jede der in § 1 Abs. 2 Satz 1 genannten Personen oder Stellen, die Daten für sich selbst speichert oder durch andere speichern läßt.
2. Dritter jede Person oder Stelle außerhalb der speichernden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich dieses Gesetzes im Auftrag tätig werden.
3. eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen ungeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren; nicht hierzu gehören Akten und Akten-sammlungen, es sei denn, daß sie durch automatisierte Verfahren ungeordnet und ausgewertet werden können.

§ 3

Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist in jeder ihrer in § 1 Abs. 1 genannten Phasen nur zulässig, wenn

1. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. der Betroffene eingewilligt hat.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen.

§ 4

Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

§ 7 Zulässigkeit der Datenverarbeitung

Die Verarbeitung . . . ,

ist . . .
nur zulässig, wenn

1. diese Anordnung oder eine staatliche oder andere kirchliche Rechtsvorschrift sie erlaubt oder
2. . . .

§ 3 Rechte des Betroffenen

gleichlautend

1. Auskunft über die zu seiner Person gespeicherten Daten.
2. Berichtigung der zu seiner Person gespeicherten Daten, wenn sie unrichtig sind.
3. Sperrung der zu seiner Person gespeicherten Daten, wenn sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen läßt oder nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung.
4. Löschung der zu seiner Person gespeicherten Daten, wenn ihre Speicherung unzulässig war oder – wahlweise neben dem Recht auf Sperrung – nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung.

§ 5

Datengeheimnis

(1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.

(2) Diese Personen sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe von Absatz 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 6

Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die in der Anlage genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation fortzuschreiben. Stand der Technik und Organisation im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Gewährleistung der Durchführung dieses Gesetzes gesichert erscheinen läßt. Bei der Bestimmung des Standes der Technik und Organisation sind

§ 4 Datengeheimnis

(1) Den im Rahmen des § 1 Abs. 2 bei der Datenverarbeitung beschäftigten Personen ist untersagt, . . .

(2) Diese Personen sind bei der Aufnahme ihrer Tätigkeit über den Inhalt des Datengeheimnisses zu belehren und auf seine Einhaltung schriftlich zu verpflichten.

Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort:

§ 5 Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 1 Abs. 2 personenbezogene Daten verarbeitet, . . .

(2) Die in der Anlage genannten Anforderungen werden nach dem jeweiligen Stand der Technik . . .

insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind.

Zweiter Abschnitt

Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

§ 7

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für Behörden und sonstige öffentliche Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für Vereinigungen solcher Körperschaften, Anstalten und Stiftungen. Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, gelten von den Vorschriften dieses Abschnittes jedoch nur die §§ 15 bis 21.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die Vorschriften dieses Abschnittes mit Ausnahmen der §§ 15 bis 21 auch für

1. Behörden und sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen.
2. Behörden und sonstige öffentliche Stellen der Länder, soweit sie als Organe der Rechtspflege tätig werden, ausgenommen in Verwaltungsangelegenheiten.

Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen und soweit sie die Voraussetzungen von Satz 1 Nr. 1 erfüllen, gelten die Vorschriften dieses Abschnittes nicht.

(3) Abweichend von den Absätzen 1 und 2 gelten anstelle der §§ 9 bis 14 die §§ 23 bis 27 entsprechend, soweit die Datenverarbeitung frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft.

§ 8

Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Abschnittes gelten für die in § 7 Abs. 1 und 2 genannten Stellen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 6 Abs. 1) sorgfältig auszuwählen.

entfällt

siehe § 1 Abs. 2

§ 6 Verarbeitung personenbezogener Daten im Auftrag

(1) Werden geschützte personenbezogene Daten im Auftrag kirchlicher Stellen durch andere Personen oder Stellen verarbeitet (vgl. § 1 Abs. 2) ist der Auftragnehmer . . .

(§ 5 Abs. 1) sorgfältig auszuwählen.

(2) Die Vorschriften dieses Abschnittes gelten mit Ausnahme der §§ 15 bis 21 nicht für die in § 7 Abs. 1 und 2 genannten Stellen, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Verarbeitung personenbezogener Daten in jeder ihrer in § 1 Abs. 1 genannten Phasen nur im Rahmen der Weisungen des Auftraggebers zulässig.

(3) Für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Bund oder einer bundesunmittelbaren Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, gelten die §§ 15 bis 21 entsprechend, soweit diese Personen oder Personenvereinigungen in den Fällen des Absatzes 1 Satz 1 im Auftrag tätig werden.

§ 9

Datenspeicherung und -veränderung

(1) Das Speichern und das Verändern personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

(2) Werden Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Aufgaben hinzuweisen.

§ 10

Datenübermittlung innerhalb des öffentlichen Bereichs

(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. 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.

(2) 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.

(2) gleichlautend mit folgender Verweisung: „Mit Ausnahme der §§ 15 bis 18 nicht für die in § 1 Abs. 2 genannten Stellen,“.

(3) gleichlautend mit Hinweis auf die „Mehrheit der Anteile den in § 1 Abs. 2 genannten Stellen“ und mit Verweisung auf §§ 15 bis 18.

§ 9 Datenspeicherung und -veränderung

gleichlautend

§ 10 Datenübermittlung innerhalb des kirchlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an die in § 1 Abs. 2 genannten Stellen ist zulässig, wenn ...

gleichlautend im übrigen mit Ausnahme des Hinweises auf § 45 S. 2 Nr. 1, S. 3 BDSG.

(2) Die Übermittlung personenbezogener Daten an kirchliche Werke und Einrichtungen, die nicht unter § 1 Abs. 2 fallen, ist in entsprechender Anwendung von Abs. 1 zulässig, sofern der Empfänger sich verpflichtet, diese Anordnung hinsichtlich der zu empfangenden Daten anzuwenden, Weisungen der übermittelnden Stelle einzuhalten und sich der Aufsicht des Datenschutzbeauftragten (§§ 15–18) zu unterstellen. Dem Empfänger ist die Übermittlung der empfangenen Daten an andere Stellen untersagt.

§ 11

Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

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. 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. Für die Übermittlung an Behörden und sonstige Stellen außerhalb des Geltungsbereichs 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.

§ 12

Veröffentlichung über die gespeicherten Daten

(1) Behörden und sonstige öffentliche Stellen geben

1. die Art der von ihnen oder in ihrem Auftrag gespeicherten personenbezogenen Daten.
2. die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist.
3. den betroffenen Personenkreis.

(3) Die Übermittlung personenbezogener Daten an Stellen anderer öffentlich-rechtlicher Religionsgesellschaften ist in entsprechender Anwendung von Abs. 1 zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden und staatliche Rechtsvorschriften dem nicht entgegenstehen.

(4) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Bundes oder eines Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen ist in entsprechender Anwendung von Abs. 1 zulässig, soweit es nach staatlichem Recht erlaubt ist und kirchliche Datenschutzbestimmungen dem nicht entgegenstehen. § 1 Abs. 4 bleibt unberührt.

§ 11 Datenübermittlung an Stellen außerhalb des kirchlichen und öffentlichen Bereiches

(1) Die Übermittlung personenbezogener Daten . . . und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

(2) § 10 Abs. 1 Satz 2 und § 10 Abs. 2 gelten entsprechend.

§ 12 Veröffentlichungen über die gespeicherten Daten

(1) Die bischöfliche Behörde gibt

1. die Art der von den in § 1 Abs. 2 genannten Stellen gespeicherten Daten und den betroffenen Personenkreis,
2. die Stellen, an die personenbezogene Daten regelmäßig übermittelt werden, sowie die Art der zu übermittelnden Daten

4. die Stellen, an die sie personenbezogene Daten regelmäßig übermitteln sowie
5. die Art der zu übermittelnden Daten unverzüglich nach der ersten Einspeicherung in dem für ihren Bereich bestehenden Veröffentlichungsblatt für amtliche Bekanntmachungen bekannt. Auf Antrag sind dem Betroffenen die bisherigen Bekanntmachungen zugänglich zu machen.

(2) Absatz 1 gilt nicht

1. für die Behörden für Verfassungsschutz, den Bundesnachrichtendienst, den militärischen Abschirmdienst sowie andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird, das Bundeskriminalamt, die Behörden der Staatsanwaltschaft und der Polizei sowie für Bundes- und Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern.
2. für die personenbezogenen Daten, die deshalb nach § 14 Abs. 2 Satz 2 gesperrt sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht nach § 14 Abs. 3 Satz 1 gelöscht werden dürfen.
3. für gesetzlich vorgeschriebene Register oder sonstige auf Grund von Rechts- oder veröffentlichten Verwaltungsvorschriften zu führende Dateien, soweit die Art der in ihnen gespeicherten personenbezogenen Daten, die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, der betroffene Personenkreis, die Stellen, an die personenbezogene Daten regelmäßig übermittelt werden, sowie die Art der zu übermittelnden Daten in Rechts- oder veröffentlichten Verwaltungsvorschriften festgelegt sind.

(3) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, für die in § 7 Abs. 1 Satz 1 genannten Behörden und sonstigen öffentlichen Stellen das Veröffentlichungsblatt sowie das Verfahren der Veröffentlichung zu bestimmen. Die Landesregierungen werden ermächtigt, durch Rechtsverordnung für die in § 7 Abs. 2 Satz 1 genannten Behörden und sonstigen öffentlichen Stellen das Veröffentlichungsblatt sowie das Verfahren der Veröffentlichung zu bestimmen.

§ 13

Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt

unverzüglich nach der ersten Einspeicherung im kirchlichen Amtsblatt für die Diözese bekannt. Auf Antrag sind dem Betroffenen die bisherigen Bekanntmachungen zugänglich zu machen.

(2) Abs. 1 gilt nicht für die personenbezogenen Daten, die deshalb nach § 14 Abs. 2 Satz 2 gesperrt sind, weil sie aufgrund gesetzlicher Vorschriften nicht nach § 14 Abs. 3 Satz 1 gelöscht werden dürfen.

(3) Abs. 1 gilt ebenfalls nicht für gesetzlich vorgeschriebene Register

§ 13 Auskunft an den Betroffenen

(1)
S. 1 und 2 gleichlautend, S. 3 entfällt.

das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht in den Fällen des § 12 Abs. 2 Nr. 1 und 2.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen,
4. die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 12 Abs. 2 Nr. 1 genannten Behörden bezieht.

(4) Die Auskunftserteilung ist gebührenpflichtig. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände und die Höhe der Gebühr näher zu bestimmen sowie Ausnahmen von der Gebührenpflicht zuzulassen. Die Gebühren dürfen nur zur Deckung des unmittelbar auf Amtshandlungen dieser Art entfallenden Verwaltungsaufwandes erhoben werden. Ausnahmen von der Gebührenpflicht sind insbesondere in den Fällen zuzulassen, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft zur Berichtigung oder Löschung gespeicherter personenbezogener Daten geführt hat. Im übrigen findet das Verwaltungskostengesetz Anwendung.

§ 14

Berichtigung, Sperrung und Löschung von Daten

- (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.
- (2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Sie sind ferner zu sperren, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen

(2) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die Erfüllung des der speichernden Stelle obliegenden kirchlichen Auftrages gefährden würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen.

(3) Die Auskunftserteilung ist gebührenpflichtig. Die Gebühren dürfen nur zur Deckung des unmittelbar auf Amtshandlungen dieser Art entfallenden Verwaltungsaufwandes erhoben werden. Eine Gebühr ist in den Fällen nicht zu erheben,

gleichlautend wie 4. Satz.

(4) Durch bischöfliche Anordnung werden das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen, die gebührenpflichtigen Tatbestände, die Höhe der Gebühr sowie Ausnahmen von der Gebührenpflicht bestimmt.

§ 14 Berichtigung, Sperrung und Löschung von Daten gleichlautend

Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt, oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene in die Nutzung eingewilligt hat.

(3) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war oder wenn es in den Fällen des Absatzes 2 Satz 2 der Betroffene verlangt.

§ 15

Durchführung des Datenschutzes in der Bundesverwaltung

Die obersten Bundesbehörden, der Vorstand der Deutschen Bundesbahn sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von einer obersten Bundesbehörde lediglich Rechtsaufsicht ausgeübt wird, haben jeweils für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, daß

1. eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger geführt und
2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.

§ 16

Allgemeine Verwaltungsvorschriften

Die obersten Bundesbehörden und der Vorstand der Deutschen Bundesbahn erlassen jeweils für ihren Geschäftsbereich allgemeine Verwaltungsvorschriften, die die Ausführung dieses Gesetzes, bezogen auf die besonderen Verhältnisse in dem jeweiligen Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, regeln.

§ 15 Durchführung des Datenschutzes

Die in § 1 Abs. 2 genannten Stellen haben jeweils für ihren Bereich die Ausführung dieser Anordnung sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, daß

1. . . . gleichlautend.

entfällt

§ 17

**Bestellung eines Bundesbeauftragten
für den Datenschutz**

(1) Es ist ein Bundesbeauftragter für den Datenschutz zu bestellen. Der Bundesbeauftragte wird auf Vorschlag der Bundesregierung vom Bundespräsidenten ernannt. Er muß bei seiner Ernennung das 35. Lebensjahr vollendet haben.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

„Ich schwöre, daß ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mit Gott helfe.“

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederbestellung ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministers des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 16 Bestellung und Rechtsstellung eines Beauftragten für Datenschutz

(1) Der Bischof bestellt für den Bereich seines Bistums einen Beauftragten für den Datenschutz. Die Bestellung erfolgt für die Dauer von drei Jahren. Wiederbestellung ist möglich. Bei Vorliegen eines wichtigen Grundes kann er von dem Bischof vorzeitig aus dem Amt entlassen werden.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Er ist auf die gewissenhafte Erfüllung seiner Amtspflichten und die Einhaltung des kirchlichen und staatlichen Rechts zu verpflichten.

(3) Der Beauftragte ist in Ausübung seines Amtes unabhängig und nur dem kirchlichen Recht und dem für die Kirchen verbindlichen staatlichen Recht unterworfen.

(4) Der Beauftragte für Datenschutz untersteht in Ausübung seines Amtes der Dienst- und Rechtsaufsicht des Bischofs.

(5) Bestellen mehrere Bischöfe einen gemeinsamen Beauftragten für den Datenschutz, untersteht er jeweils der Rechtsaufsicht desjenigen Bischofs, in dessen Diözese er in Erfüllung seines Auftrages tätig wird; er untersteht der Dienstaufsicht des Bischofs, in dessen Bistum er angestellt ist.

(6) Der Beauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Der Beauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung seines Dienstherrn weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen.

(7) Die Genehmigung, als Zeuge auszusagen, soll in der Regel erteilt werden.

§ 18

**Rechtsstellung des Bundesbeauftragten
für den Datenschutz**

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlich demokratischen Grundordnung für deren Erhaltung einzutreten.

(5) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten,

kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 3. Februar 1971 (BGBl. I S. 105), geändert durch das Einführungsgesetz zum Strafgesetzbuch vom 2. März 1974 (BGBl. I S. 469), bleibt unberührt.

(6) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Siebente Gesetz zur Änderung beamtenrechtlicher und besoldungsrechtlicher Vorschriften vom 20. Dezember 1974 (BGBl. I S. 3716), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt.

§ 19

Aufgaben des Bundesbeauftragten für den Datenschutz

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den in § 7 Abs. 1 genannten Behörden und sonstigen öffentlichen Stellen des Bundes, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die Bundesregierung und einzelne Minister sowie die übrigen in § 7 Abs. 1 genannten Behörden und sonstigen Stellen in Fragen des Datenschutzes beraten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Außerdem erstattet er dem Deutschen Bundestag jährlich, erstmals zum 1. Januar 1979 einen Tätigkeitsbericht. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses des Deutschen Bundestages oder der Bundesregierung kann der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen. Der Beauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

§ 17 Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wacht über die Einhaltung der Vorschriften dieser Anordnung sowie anderer Vorschriften über den Datenschutz. Zu diesem Zweck kann er Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die bischöfliche Behörde und sonstige kirchliche Dienststellen in seinem Bereich in Fragen des Datenschutzes beraten. Auf Anforderung der bischöflichen Behörde hat der Beauftragte Gutachten zu erstellen und Berichte zu erstatten.

(2) Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, den Beauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. 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;
2. während der Dienstzeit Zutritt zu allen Diensträumen, die der Verarbeitung und Aufbewahrung automatisierter Dateien dienen, zu gewähren,

(3) Die in Absatz 1 Satz 1 genannten Behörden und sonstigen Stellen sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren 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,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die Sätze 1 und 2 gelten für die in § 12 Abs. 2 Nr. 1 genannten Bundesbehörden mit der Maßgabe, daß die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders damit betrauten Beauftragten zu gewähren ist. Satz 2 gilt für die in § 12 Abs. 2 Nr. 1 genannten Bundesbehörden nicht, soweit die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet.

(4) Der Bundesbeauftragte führt ein Register der automatisch betriebenen Dateien, in denen personenbezogene Daten gespeichert werden. Das Register kann von jedem eingesehen werden. Die in Absatz 1 Satz 1 genannten Behörden und sonstigen Stellen sind verpflichtet, die von ihnen automatisch betriebenen Dateien beim Bundesbeauftragten anzumelden. Das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der militärische Abschirmdienst sind von der Meldepflicht ausgenommen. Zu den Dateien der übrigen in § 12 Abs. 2 Nr. 1 genannten Bundesbehörden wird ein besonderes Register geführt. Es beschränkt sich auf eine Übersicht über Art und Verwendungszweck. Satz 2 findet auf dieses Register keine Anwendung. Das Nähere regelt der Bundesminister des Innern durch Rechtsverordnung.

(5) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den Behörden und sonstigen öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 30 hin.

§ 20

Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder

soweit nicht sonstige kirchliche Vorschriften entgegenstehen.

(3) Der Beauftragte führt ein Register der automatisch betriebenen Dateien, in denen personenbezogene Daten gespeichert werden. Das Register kann von jedermann eingesehen werden. Die in § 1 Abs. 2 genannten Stellen sind verpflichtet, die von ihnen automatisch betriebenen Dateien beim zuständigen Beauftragten anzumelden.

(4) Der Beauftragte wirkt auf die Zusammenarbeit mit den kirchlichen Stellen, die im Geltungsbereich dieser Anordnung Aufgaben des Datenschutzes wahrnehmen, insbesondere mit den anderen kirchlichen Beauftragten für den Datenschutz hin.

(5) Zu seinem Aufgabenbereich gehört die Zusammenarbeit mit den staatlichen Beauftragten für den Datenschutz.

§ 19 Beanstandungen durch den Beauftragten für den Datenschutz

(1) Stellt der Beauftragte für den Datenschutz Verstöße gegen die Vorschriften dieser Anordnung oder gegen andere Datenschutzbestimmungen oder

sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
2. bei der Bundesbahn gegenüber dem Vorstand,
3. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 3 unterrichtet der Bundesbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Bundesbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 3 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 21

Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch die in § 7 Abs. 1 genannten Behörden oder sonstigen öffentlichen Stellen des Bundes, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein.

sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies gegenüber der zuständigen obersten Behörde und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden angemessenen Frist auf.

(2)

(3)

(4)

gleichlautend

Der letzte Satz von Abs. 4 entfällt.

§ 18 Anrufung des Beauftragten für den Datenschutz

Jedermann kann sich an den zuständigen Beauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch die in § 1 Abs. 2 genannten Stellen in seinen Rechten verletzt worden zu sein.

§ 20 Schlußbestimmung

(1) Der Bischof erläßt die zur Ausführung dieser Anordnung erforderlichen Bestimmungen.

(2) Diese Anordnung tritt zum 1. September 1978 in Kraft. § 5 und die Anlage zu § 5 Abs. 2 S. 1 treten zum 1. Januar 1979 in Kraft.

3.3 **Datenschutz und Verwendung personenbezogener Angaben für Forschungszwecke** – Grundsätze und Richtlinien, vorgelegt im Auftrag der European Science Foundation¹³⁾

Präambel

Die Notwendigkeit, den einzelnen vor den Gefahren einer Verarbeitung seiner personenbezogenen Daten zu schützen, ist in den vergangenen Jahren sowohl auf nationaler wie auf internationaler Ebene wiederholt betont worden. Dies gilt insbesondere für Länder mit Wissenschaftsorganisationen, die Mitglieder der European Science Foundation sind. Österreich und Portugal haben den Datenschutz ausdrücklich in ihren Verfassungen verankert. In der Bundesrepublik Deutschland, Dänemark, Frankreich, Norwegen, Österreich und Schweden sind spezielle Datenschutzgesetze in Kraft. Gesetzesentwürfe werden zur Zeit in Belgien, der Schweiz und Spanien beraten, während offizielle Gutachten zu dieser Thematik in Großbritannien und den Niederlanden vorliegen. Auf internationaler Ebene sind ebenfalls beachtliche Aktivitäten entfaltet worden. So hat der Europarat erst kürzlich eine Konvention zum Schutz von Personen unter besonderer Berücksichtigung der automatischen Verarbeitung personenbezogener Daten erarbeitet, während die OECD-Richtlinien über den Schutz der Privatheit und den grenzüberschreitenden Datenverkehr vorgelegt hat. Besondere Aufmerksamkeit verdienen auch die im Rahmen der Kommission der Europäischen Gemeinschaften geführten Diskussionen über eine mögliche Richtlinie sowie die Entschließung des Europäischen Parlaments, in der unverzügliche Entscheidungen gefordert wurden.

Die Anwendung der Datenschutzgesetze hat jedoch zunehmend zu Einschränkungen bei der Verwendung personenbezogener Daten für die wissenschaftliche Forschung geführt. Hinzuweisen ist besonders auf die Schwierigkeit bei der Auswertung von Informationsbeständen der öffentlichen Verwaltung, vor allem der den statistischen Ämtern zur Verfügung stehenden Angaben, sowie auf die Konsequenzen für die wissenschaftliche Forschung, wenn die Behörden personenbezoge-

ne Daten vernichten, nachdem diese Angaben für den Zweck, für den sie erhoben worden sind, nicht mehr gebraucht werden. Diese Entwicklung war Anlaß für die im August 1977 verabschiedeten Bellagio Principles sowie für die im August 1978 von der IFDO (International Federation of Data Organisations) in Köln veranstaltete internationale Konferenz über Datenschutz und den Bedarf der Sozialforschung nach Datenzugang.

Angesichts dieser Situation und unbeschadet der Verpflichtung zum Respekt vor der persönlichen Integrität, die auch hier erneut nachdrücklich bekräftigt wird, sind bereichsspezifische Regelungen erforderlich, um elementare Voraussetzungen wissenschaftlicher Forschung sicherzustellen. Die folgenden Prinzipien und Richtlinien sind deshalb in der Hoffnung aufgestellt worden, mit ihrer Hilfe eine gesetzliche Regelung erarbeiten zu können, die sowohl den Schutz personenbezogener Daten als auch die Notwendigkeit des Zugangs zu solchen Angaben für Forschungszwecke gleichermaßen gewährleisten.

Grundsätze

- 1.1 Unter „personenbezogene Daten“ sind im Rahmen dieses Dokuments in Übereinstimmung mit der auch von der OECD übernommenen Definition einer Expertengruppe des Europarats für den Datenschutz alle Angaben zu verstehen, die sich auf eine bestimmte oder bestimmbare Person beziehen.
- 1.2 Die Datenschutzgesetzgebung muß, um ihrer Aufgabe, die Integrität des einzelnen zu schützen, gerecht zu werden, jegliche Verarbeitung personenbezogener Angaben regeln und deshalb auch die Verarbeitung für Forschungszwecke.
- 1.3 Standesnormen sind als Ergänzung der erforderlichen legislativen Maßnahmen auf dem Gebiet des Datenschutzes zu sehen. Die zuständigen wissenschaftlichen Organisationen sollten deshalb die Entwicklung solcher Normen anregen, um mit ihrer Hilfe den spezifischen Bedürfnissen der unterschiedlichen Disziplinen im Rahmen der gesetzlich definierten Verarbeitungsbedingungen Rechnung zu tragen.
- 1.4 Die Freiheit der Forschung setzt den größtmöglichen Zugang zur Information voraus. Die Gesetzgebung sollte deshalb nicht nur die Rahmenbedingungen für die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung

¹³⁾ Dieser Entwurf ist von einer Unterkommission der European Science Foundation, Straßburg, unter Vorsitz des Hessischen Datenschutzbeauftragten erarbeitet und am 7. November 1979 der Generalversammlung der European Science Foundation zur weiteren Beratung vorgelegt worden. Der hier veröffentlichte Text ist eine Übersetzung des englischen Originals.

regeln, sondern auch den Zugang zu den erforderlichen Informationen sicherstellen.

1.5 Die wissenschaftliche Forschung sollte im Sinne einer gegenwärtig weitgehend akzeptierten und praktizierten Forderung soweit wie möglich mit anonymisierten Daten auskommen, um den Datenschutz zu gewährleisten.

1.6 Wissenschaftsorganisationen und Berufsvereinigungen sollten in Zusammenarbeit mit öffentlichen Stellen die weitere Entwicklung von Anonymisierungstechniken und -verfahren fördern. Anonymität im Sinne dieser Grundsätze und Richtlinien ist dann als gegeben anzusehen, wenn eine Person nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Personal identifiziert werden kann (sog. faktische Anonymisierung).

Richtlinien

2.1 Jede Verarbeitung personenbezogener Daten für Forschungszwecke setzt entweder eine ausdrückliche gesetzliche Ermächtigung oder die informierte Einwilligung des Betroffenen voraus.

2.2 Eine informierte Einwilligung liegt dann vor, wenn die Betroffenen ausdrücklich und deutlich darüber aufgeklärt worden sind:

- a) daß die Datenerhebung freiwillig ist und die Verweigerung der Teilnahme an einer Untersuchung keine Maßnahmen gegen den Betroffenen zur Folge hat;
- b) über Zweck und Gegenstand des Forschungsprojekts;
- c) durch wen und für wen die Daten gesammelt werden;
- d) daß die erhobenen Daten ausschließlich für Zwecke wissenschaftlicher Forschung verarbeitet werden.

2.3 Von einer informierten Einwilligung sollte mit Genehmigung der für den Datenschutz verantwortlichen staatlichen Kontrollinstanz nur dann abgesehen werden, wenn:

- a) wichtige Forschungsziele in Frage gestellt würden;
- b) die Information den Betroffenen psychisch oder physisch gefährden könnte.

2.4 Die für den Datenschutz verantwortliche staatliche Kontrollinstanz sollte auch

berechtigt sein, die Einwilligungsbedingungen abzuändern oder auch ganz auf die Mitwirkung des Betroffenen zu verzichten, wenn:

- a) bereits erhobene personenbezogene Daten Dritten zu Forschungszwecken übermittelt werden sollen;
- b) eine Einwilligung für die erneute Verwendung bereits erhobener Daten entweder mit Rücksicht auf Nachteile oder Schäden für den Betroffenen nicht angebracht erscheint oder aber die Forschungsziele nicht mehr verwirklicht werden könnten, insbesondere aus Zeitgründen oder im Hinblick auf außergewöhnliche Kosten.

2.5 Personenbezogene Daten, die nicht für Forschungszwecke gespeichert werden, sollten der Forschung nicht ohne die informierte Einwilligung des Betroffenen zugänglich sein, es sei denn, der Empfänger ist nicht in der Lage, die Daten auf eine bestimmte Person zu beziehen. Ausnahmen gelten in den Fällen der Ziffern 2.3 und 2.4 der Richtlinien.

2.6 Soweit die Verarbeitung ausschließlich dazu dient, Stichproben für die wissenschaftliche Forschung zu ziehen, sollten Behörden Daten wie Name, Adresse, Geburtsdatum und Geschlecht, die sie zu anderen als Forschungszwecken erhoben und gespeichert haben, ohne Rücksicht auf Gegenstand und Zweck der Forschung und ohne die Einwilligung des Betroffenen zur Verfügung stellen. Dazu bedarf es jedoch einer ausdrücklichen gesetzlichen Ermächtigung oder eines rechtlich gleichwertigen Verfahrens.

2.7 Personenbezogene Daten, die für Forschungszwecke erhoben worden sind, sollten nicht für andere Zwecke verarbeitet werden.

2.8 Insbesondere sollten personenbezogene Daten, die für Forschungszwecke gespeichert werden, nicht zu Maßnahmen oder Entscheidungen gegen den Betroffenen verwandt werden. Dies gilt nicht im Zusammenhang der wissenschaftlichen Forschung selbst, oder soweit eine ausdrückliche Ermächtigung des Betroffenen vorliegt.

2.9 Personenbezogene Daten aus dem Bereich wissenschaftlicher Forschung dürfen nur mit Zustimmung der Betroffenen an Dritte zu Forschungszwecken übermittelt werden, es sei denn, der Betroffene ist für

den Empfänger nicht bestimmbar. Ausnahmen gelten lediglich für die in 2.3 und 2.4 geregelten Fälle.

Personenbezogene Forschungsdaten sollen nur mit ausdrücklicher Zustimmung der Betroffenen in personenbezogener Form veröffentlicht werden.

- 2.11 Das Recht des einzelnen, Gewißheit darüber zu erhalten, ob Daten über ihn gespeichert werden, die Richtigkeit der ihn betreffenden Daten zu bestreiten, Löschung, Berichtigung, Vervollständigung oder Ergänzung zu verlangen, sollte auf Forschungsprojekte beschränkt werden, bei denen die Datenverarbeitung in personenbezogener Form beabsichtigt ist.
- 2.12 Die Leiter von Forschungsprojekten, in deren Kontext personenbezogene Daten verarbeitet werden, sollten für die notwendigen, jeweils dem letzten wissenschaftlichen und technischen Stand der Entwicklung angepaßten technischen und organisatorischen Maßnahmen der Datensicherung verantwortlich sein.
- 2.13 Jeder, der sich an einem Forschungsprojekt beteiligt, bei dem personenbezogene Daten verarbeitet werden, sollte schriftlich auf das Datengeheimnis verpflichtet werden.
- 2.14 Um die Anwendung dieser Grundsätze und Richtlinien sicherzustellen, soll ein Register eingerichtet werden, das sowohl die jeweiligen Organisationen verzeichnet, die Forschungsprojekte mit personenbezogenen Daten fördern oder durchführen, als auch die einzelnen Forschungsprojekte selbst.
- 2.15 Die für den Datenschutz verantwortliche staatliche Kontrollinstanz sollte dieses Register einrichten und insbesondere dafür sorgen, daß die notwendigen technischen und organisatorischen Maßnahmen der Datensicherung ergriffen werden.
- 2.16 Soweit der Zweck eines bestimmten Forschungsprojekts, für das personenbezogene Daten gespeichert worden sind, erfüllt ist, sollten die Angaben anonymisiert und die erforderlichen Maßnahmen der Datensicherung ergriffen werden, etwa eine Speicherung von Identifikatoren bei einem zentralen Forschungsarchiv.
- 2.17 Die Entscheidung, personenbezogene Daten zu vernichten, die sich bei öffentlichen Stellen befinden, sollte nur nach Berücksichtigung ihrer möglichen zukünftigen Verarbeitung für Forschungszwecke und im Einvernehmen mit dem zentralen Datenarchiv oder einer ähnlichen Organisation getroffen werden.