LANDTAG RHEINLAND-PFALZ
11. Wahlperiode

Drucksache 11/3427
21. 12. 1989

Unterrichtung

durch die Datenschutzkommission

Zwölfter Tätigkeitsbericht nach § 21 des Landesdatenschutzgesetzes – LDatG – für die Zeit vom 1. Oktober 1987 bis 30. September 1989

Inhaltsübersicht

Dem Präsidenten des Landtags mit Schreiben vom 19. Dezember 1989 zugeleitet.

Druck: Landtag Rheinland-Pfalz, 31. Januar 1990

Abkürzungen:

ISM	Ministerium des Innern und für Sport
FM	Ministerium der Finanzen
JM	Ministerium der Justiz
MSF	Ministerium für Soziales und Familie
MLWF	Ministerium für Landwirtschaft, Weinbau und Forsten
MWV	Ministerium für Wirtschaft und Verkehr
KM	Kultusministerium
MUG	Ministerium für Umwelt und Gesundheit

Tätigkeitsberichte der Datenschutzkommission

1. Tätigkeitsbericht Drs. 7/3342	v. 17. Oktober 1974
2. Tätigkeitsbericht Drs. 8/350	v. 1. Oktober 1975
3. Tätigkeitsbericht Drs. 8/1444	v. 1. Oktober 1976
4. Tätigkeitsbericht Drs. 8/2470	v. 10. Oktober 1977
5. Tätigkeitsbericht Drs. 8/3492	v. 12. Oktober 1978
6. Tätigkeitsbericht Drs. 9/253	v. 15. Oktober 1979
7. Tätigkeitsbericht Drs. 9/970	v. 15. Oktober 1980
8. Tätigkeitsbericht Drs. 9/1869	v. 28. Oktober 1981
9. Tätigkeitsbericht Drs. 10/270	v. 26. Oktober 1983
10. Tätigkeitsbericht Drs. 10/1922	v. 8. November 1985
11. Tätigkeitsbericht Drs. 11/710	v. 11. Dezember 1987

1 Vorbemerkung

„Da zu erwarten ist, daß in naher Zukunft die Datenschutzkommission durch einen Datenschutzbeauftragten abgelöst oder ersetzt wird . . ." Dieser Satz, der den vor zwei Jahren vorgelegten 11. Tätigkeitsbericht der Datenschutzkommission (DSK) einleitete, kann heute wiederholt werden. Die damit angesprochene organisationsrechtliche Zäsur der Datenschutzarbeit steht noch aus. Die DSK hatte noch einmal Gelegenheit darzutun, daß unabhängige Datenschutzkontrolle auch durch ein Kollegialorgan wirksam ausgeübt werden kann.

Entgegen allen Erwartungen wächst mit dem zeitlichen Abstand zum Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983 das datenschutzrechtliche Konfliktpotential. Dies hat mehrere Ursachen. Die wichtigste ist wohl, daß den Anforderungen des Bundesverfassungsgerichts an die gesetzgeberische Weiterentwicklung des Datenschutzes noch immer nicht in genügendem Umfange entsprochen ist. Am ehesten haben noch die Länder mit der Schaffung bereichsspezifischer Datenschutzvorschriften – vereinzelt auch mit der Novellierung von Datenschutzgesetzen – Folgerungen aus der verfassungsrechtlichen Neuorientierung gezogen. Im Bund beschränkte man sich lange Zeit auf Lösungsversuche auf der Grundlage des kleinsten gemeinsamen Nenners. Nach Lage der Dinge ist voraussichtlich auch in dieser Wahlperiode des Deutschen Bundestages nicht mehr mit einer Novellierung des Bundesdatenschutzgesetzes (BDSG) zu rechnen. Dabei geht es keineswegs nur um dieses Gesetz, sondern auch um die Novellierung von Gesetzen durchaus vergleichbarer Bedeutung, wie z. B. die Strafprozeßordnung (StPO) oder die Sicherheitsgesetze.

Das Ausbleiben der gesetzgeberischen Reaktion auf die Entscheidung des Bundesverfassungsgerichts wirft seinerseits verfassungsrechtliche Probleme auf. Selbst bei Anlegung eines großzügigen Maßstabs fällt es schwer, die weitere Ausdehnung der Übergangsfristen zur Beseitigung von Regelungsdefiziten, die das Bundesverfassungsgericht dem Gesetzgeber grundsätzlich zubilligt, noch zu rechtfertigen. Mehrere Gerichte haben deutlich darauf hingewiesen, daß die Schaffung verfassungsmäßiger Grundlagen für Informationseingriffe keinen weiteren Aufschub verträgt. In dieser Situation sollte der Landesgesetzgeber nicht länger zögern, die Novellierung des Landesdatenschutzgesetzes (LDatG) in Angriff zu nehmen, zumal die Strukturelemente eines neuen Datenschutzrechts in einigen Ländergesetzen verwirklicht sind.
Bisweilen könnte der Eindruck entstehen, als nutze die Verwaltung diese Zeit des Übergangs, die zugleich auch eine Zeit der Rechtsunsicherheit ist, mit einer längerfristigen Zielsetzung: Sie will eine durch Datenschutzrestriktionen bestimmte Realität schaffen in der Erwartung, daß diese später vom Gesetzgeber bestätigt wird. Der Widerstand gegen eine Erstreckung der Datenschutzkontrolle auf Akten sowie das Bestreiten der von der DSK in Anspruch genommenen Zuständigkeit für die Kontrolle der Einhaltung „anderer Vorschriften über den Datenschutz" (§ 17 Abs. 1 LDatG) sind Beispiele hierfür.

Das Problem läßt sich indessen auch von einer anderen Seite beleuchten. Die stetige Verbesserung des Preis-Leistungsverhältnisses im Technikeinsatz hat zur Folge, daß die automatisierte Datenverarbeitung auch in der öffentlichen Verwaltung in einem vor wenigen Jahren noch kaum vorstellbaren Umfange eingesetzt wird. Alleine die Sachkosten für die Automation im Landesbereich liegen pro Jahr wohl bei 100 Mio. DM, nimmt man den Kommunalbereich hinzu, dürfte die 200 Mio. DM-Grenze weit überschritten sein. In gleichem Maße wachsen die Rationalisierungserwartungen, die freilich in dem gewünschten Maße nur dann zu realisieren sind, wenn herkömmliche Informationsstrukturen verändert werden. Die Datenschutzkontrolle hat die hieraus entstehenden Probleme mit einem rechtlichen Instrumentarium zu lösen, das nicht mehr angemessen ist. Dementsprechend fehlt es einerseits an gesetzlichen Vorgaben, andererseits muß verhindert werden, daß durch die Nutzung der Datenverarbeitungstechnik persönlichkeitsgefährdende Entwicklungen eingeleitet werden, die nicht mehr umkehrbar sind. Die vor diesem Hintergrund zur Vorsicht und Zurückhaltung mahnenden Empfehlungen der DSK werden gelegentlich als grundsätzliche Ablehnungshaltung mißdeutet.

Wenn in diesen Tagen viel von der Ausstrahlungskraft und der Faszination der Freiheit die Rede ist, dann sind damit – wohl in erster Linie – die politischen Freiheitsrechte der Bürger gemeint. Im Zeitalter der automatisierten Datenverarbeitung ist ein grundlegend wichtiger Teil dieser Freiheitsrechte das Recht auf Datenschutz, informationelle Selbstbestimmung und Teilhabe an Informationen als freiheitssicherndes Korrelat zum technischen Fortschritt. In diesem Sinn hat die DSK ihre Tätigkeit als Beitrag zur Sicherung und Fortentwicklung unserer demokratischen Ordnung verstanden, ohne daß damit allerdings andere staatliche Tätigkeiten beeinträchtigt werden dürfen, die ihrerseits zum Schutz dieser freiheitlichen Gesellschaft und ihres Staates erforderlich sind.

Nicht jedes in diesem Tätigkeitsbericht geschilderte Detail der Kommissionsarbeit macht diese grundsätzliche Dimension deutlich. Es ergibt sich dennoch, so hofft die DSK jedenfalls, ein Mosaik, das aufzeigt, daß in nahezu jedem Bereich staatlichen Handelns Datenschutzaspekte zu berücksichtigen sind. In der Zusammenschau zeigt sich, daß die Verwaltung innovationsfähig und sensibel genug ist, um die schutzwürdigen Bürgerbelange bei aller Aufgeschlossenheit für die Nutzung moderner Techniken angemessen zu berücksichtigen.

2 Anforderungen an das allgemeine Datenschutzrecht

2.1 Novellierung des Bundesdatenschutzgesetzes

Ende November 1987 – fast vier Jahre nach der grundlegenden Entscheidung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht im sog. „Volkszählungsurteil" – wurde vom Bundesminister des Innern der Entwurf für ein Artikelgesetz zur Neufassung des BDSG und zur Änderung des Verwaltungsverfahrensgesetzes (VwVfG) zunächst als Referentenentwurf vorgelegt. Die vorgesehenen Regelungen entsprachen inhaltlich im großen und ganzen den alten Entwürfen der Koalitionsparteien und der Bundesregierung aus der 10. Wahlperiode und wurden damit in wesentlichen Teilen den Vorstellungen des Bundesverfassungsgerichtes nicht gerecht. Die zu den alten Entwürfen bereits geäußerte Kritik der Datenschutzbeauftragten des Bundes und der Länder (DSB), wie sie in der gemeinsamen Entschließung vom März 1986 dargestellt worden war, blieb also weitgehend aktuell.

In der vom ISM erbetenen Stellungnahme bedauerte die DSK schon damals den eingetretenen Zeitverlust und wies deutlich darauf hin, daß dieser Entwurf in bestimmten Teilen dem Volkszählungsurteil (VZU) nicht entspreche. Neben einer Reihe von Einzelvorschlägen konzentrierte sich die Kritik der DSK auf das Festhalten an dem durch die Rechtsentwicklung überholten Dateibezug sowie auf die als Rückschritt bezeichnete neue Definierung der Kontrollbefugnisse des Bundesbeauftragten im Vergleich zu der fast bundesweit geübten Kontrollpraxis.

Weitere Punkte betrafen das Abrufverfahren, die Übermittlung von Daten an nichtöffentliche Stellen, die Bestellung behördlicher Datenschutzbeauftragter und den Auskunftsbereich. Die am 26. Januar 1988 dem ISM übermittelte Stellungnahme der DSK stimmte in ihren Forderungen und in ihrer Kritik weitgehend mit Stellungnahmen anderer Datenschutzbeauftragter und des Bundesbeauftragten überein; in entscheidenden Punkten fand sie Eingang in die Entschließung, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter dem turnusmäßigen Vorsitz der DSK Rheinland-Pfalz am 6. Juni 1988 mit der Gegenstimme Bayerns beschlossen hat. Hingewiesen wurde auch auf die mangelhaft ausgestaltete Zweckbindung, auf das Fehlen von Regelungen auf dem Gebiet der modernen Informations- und Kommunikationstechnik sowie auf die Gefahr der Rechtszersplitterung, nachdem in Hessen, Bremen und Nordrhein-Westfalen bereits Gesetze mit wesentlich weitergehenden Regelungen in Kraft getreten waren.

Dem Bundesminister des Innern wurde die Entschließung am 7. Juni 1988 mitgeteilt.

Von all dem unbeeindruckt wurde im materiellen Gehalt unverändert der Regierungsentwurf zum Jahresende 1988 im Bundesrat eingebracht (Bundesratsdrucksache 618/88 vom 30. Dezember 1988), wobei in der Tagespresse die Kritik bei weitem überwog.

Angesichts der kurz bevorstehenden Beratungen im Bundesrat bat die DSK den Innenminister des Landes mit Schreiben vom 20. Januar 1989, seinen Einfluß geltend zu machen, „um den Entwurf der eindeutigen Rechtsprechung des Bundesverfassungsgerichts und der modernen Rechtsentwicklung auf dem Gebiete des Grundrechtsschutzes beim Recht auf informationelle Selbstbestimmung anzupassen". Auf die wesentlichen Punkte, insbesondere auf die Gefahr der Rechtszersplitterung und auf die dringend gebotene Erweiterung des Anwendungsbereichs der materiellen datenschutzrechtlichen Regelungen über die Dateien hinaus, wurde erneut hingewiesen. Inzwischen hatte das Bundesverfassungsgericht in einem Beschluß vom 9. März 1988 (BVerfGE 78,77 ff.) unmißverständlich klargestellt, daß das Recht auf informationelle Selbstbestimmung nicht nur bei Datenerhebung unter Auskunftszwang und bei Anwendung der automatisierten Datenverarbeitung eingreift, sondern generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten schützt, also auch außerhalb des jeweiligen Anwendungsbereichs der Datenschutzgesetze des Bundes und der Länder.

Die Beratung in der 597. Sitzung des Bundesrates am 10. Februar 1989 brachte eine Vielzahl entscheidender Änderungsvorschläge, die mit wechselnden Mehrheiten angenommen wurden. So soll u. a. nunmehr sichergestellt sein, „daß auch die nichtdateimäßige Datenverarbeitung (in Akten und sonstigen amtlichen Unterlagen), soweit sie gesetzlich geregelt ist, der uneingeschränkten Kontrolle des Bundesbeauftragten für den Datenschutz unterliegt" (Bundestagsdrucksache 11/4306, S. 78, Begründung zu Nr. A 33 zu §§ 22 Abs. 1 BDSG).

Eine Reihe von Verbesserungen in den Beschlüssen des Bundesrates geht auf Anträge des Landes Rheinland-Pfalz (ISM sowie JM) zurück. Die DSK begrüßt dies ausdrücklich. Die Beschlüsse des Bundesrates insgesamt wurden von der Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 5./6. April 1989 (bei Stimmenthaltung des Bayerischen Landesbeauftragten) als Bestätigung ihrer bisher vertretenen Auffassung begrüßt. Die DSK hat auch dieser Entschließung zugestimmt. Sie hofft, daß der Gesetzentwurf mit der gebotenen Nachbesserung ohne weitere Verzögerung verabschiedet wird.

2.2 Novellierung des Landesdatenschutzgesetzes

Nachdem nunmehr sechs Jahre seit dem Volkszählungsurteil des Bundesverfassungsgerichtes vergangen sind und nachdem in Hessen, Bremen und in Nordrhein-Westfalen bereits seit Jahren Landesdatenschutzgesetze in Kraft sind, die sich an der Auslegung des informationellen Selbstbestimmungsrechtes durch das Bundesverfassungsgericht orientieren, und in weiteren Bundesländern entsprechende Gesetzentwürfe eingebracht wurden, ist es nach Auffassung der DSK dringend geboten, nunmehr auch das Landesdatenschutzgesetz zu novellieren. In Rheinland-Pfalz liegt ein vor zweieinhalb Jahren von der Fraktion der SPD in den Landtag eingebrachter Entwurf für eine Neufassung des Landesdatenschutzgesetzes vor. Spätestens bei der parlamentarischen Behandlung des von der Landesregierung ebenfalls eingebrachten Gesetzentwurfs sollten daher auch die notwendigen materiellen Regelungen getroffen werden, zumal das neue Bundesdatenschutzgesetz in dieser Wahlperiode des Bundestages voraussichtlich nicht mehr verabschiedet wird.

In Rheinland-Pfalz ist bereichsspezifischer Datenschutz zwar beispielgebend rasch und in einer größeren Zahl von Einzelgesetzen (wie z. B. Polizeiverwaltungsgesetz, Landesverfassungsschutzgesetz, Landesstatistikgesetz, Krankenhaus- und Schulgesetz) verwirklicht worden. Dennoch macht sich das Fehlen eines den Forderungen des Bundesverfassungsgerichts entsprechenden allgemeinen Datenschutzrechts im Lande doch in zunehmendem Maße bei der Rechtsanwendung in der Praxis bemerkbar. Ein großer Teil datenschutzrelevanter Vorgänge ist nach wie vor durch bereichsspezifische Regelungen nicht abgedeckt. Insoweit führt die Anwendung des geltenden Landesdatenschutzgesetzes unter Berücksichtigung der Grundsätze des Bundesverfassungsgerichts nicht selten zu unterschiedlichen Rechtsstandpunkten, die akzeptable und praktikable Lösungen erschweren.

Die DSK hat im Mai 1989 den Minister des Innern auf die geschilderten Notwendigkeiten hingewiesen und gleichzeitig ihrerseits Grundsätze dargestellt, die für eine Neufassung des Landesdatenschutzgesetzes maßgebend sein könnten. Die Grundsätze sind nachstehend wiedergegeben. Sie erheben keinen Anspruch auf Vollständigkeit, so daß weitere Vorschläge im Gesetzgebungsverfahren vorbehalten bleiben.

2.2.1 Wesentliche Grundsätze

Als unverzichtbare Regelungen für eine verfassungskonforme und wirksame Verwirklichung des Rechts auf informationelle Selbstbestimmungen werden angesehen:

a) die Einbeziehung der in Akten verarbeiteten personenbezogenen Daten,

b) die Verwirklichung einer größeren Transparenz der Datenverarbeitung,

c) die Einbeziehung der Erhebung in das allgemeine Datenschutzrecht und ihre bürgerfreundliche Ausgestaltung,

d) eine konsequente Zweckbindung für personenbezogene Daten,

e) eine präzise und umfassende Ausgestaltung der Kontrollbefugnisse,

f) eine ebenso ausgewogene Regelung der Datenverarbeitung für wissenschaftliche Zwecke unter Berücksichtigung der bisherigen Erfahrungen in der Praxis.

Zu a):
Wie bereits mehrfach von der DSK dargestellt und auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt gefordert, ist ein weiteres – auch teilweises – Festhalten am Dateibezug beim gegenwärtigen Stand der Rechtsentwicklung nicht mehr möglich. In Rheinland-Pfalz selbst wurde in einer Reihe von nach dem Volkszählungsurteil erlassenen Gesetzen die Unterscheidung von personenbezogenen Daten, die in Dateien und außerhalb derselben, insbesondere in Akten, verarbeitet werden, aufgegeben. Als Beispiele zu nennen sind hier die Informationsbestimmungen im Polizeiverwaltungsgesetz, im Verfassungsschutzgesetz, im Schulgesetz, Krankenhausgesetz und im Statistikgesetz. Den gleichen Weg sind die bereits novellierten Landesdatenschutzgesetze von Hessen, Bremen und Nordrhein-Westfalen gegangen. Auch der Bundesrat hat in seiner Stellungnahme zum Regierungsentwurf eines Bundesdatenschutzgesetzes einen Schritt in diese Richtung getan (Bundesratsdrucksache 618/88). Das Bundesverfassungsgericht hat seine Rechtsprechung zum informationellen Selbstbestimmungsrecht inzwischen eindeutig dahin konkretisiert, daß die Datenverarbeitung außerhalb von Dateien davon nicht ausgenommen sein kann (BVerfGE v. 9. März 1988, 1 Bvl 49/86, Bd.78,77ff.).

Dies entspricht auch dem aktuellen Rechtsbewußtsein der Bürger, wie es in den der DSK zugehenden Eingaben zum Ausdruck kommt.

Es steht außer Frage, daß es nicht vertretbar ist, einen wesentlichen Teil der Persönlichkeitsrechte des Bürgers von der Verarbeitungsform seiner Daten abhängig zu machen.

Zu b):
Die grundsätzliche Forderung nach hinreichender Transparenz der Datenverarbeitung für den Bürger wird vom Bundesverfassungsgericht in seinem Volkszählungsurteil erhoben. Der Bürger soll nach Möglichkeit jederzeit erkennen können, wer welche Daten über ihn speichert und zu welchem Zweck dies geschieht. Eine folgerichtige Berücksichtigung dieses Grundsatzes in der Gesetzgebung darf nicht dazu führen, daß notwendige Verwaltungsabläufe in ihrer Wirksamkeit spürbar beeinträchtigt werden.

Die so gebotene Transparenz der Datenverarbeitung sollte durch folgende Regelungen verwirklicht werden:

- Die direkte Befragung des Bürgers sollte die Regel sein; ihr muß ausdrücklich der Vorrang vor der Informationsermittlung bei dritten Personen oder Stellen eingeräumt werden.

- Die Datenerhebung beim Betroffenen muß dessen ausreichende Information über Freiwilligkeit oder Auskunftsverpflichtung, aber auch über den Zweck der Datenerhebung sowie die beabsichtigten Datenübermittlungen über den oder die Empfänger voraussetzen.

- Die Auskunftserteilung an den Betroffenen ist auf den Zweck und die Rechtsgrundlage der Speicherung auszudehnen, da er nur so in die Lage versetzt wird, seine Rechte geltend zu machen.

- Dem Grunde nach ist auch ein Recht des Betroffenen auf Einsicht in zu seiner Person geführte Akten – auch außerhalb des Verwaltungsverfahrens – zu regeln. Bei der näheren Ausgestaltung ist allerdings dieses Recht mit den oben genannten Belangen unter Berücksichtigung rechtsstaatlicher Gebote (wie berechtigte Geheimhaltung, notwendiges Funktionieren der Verwaltung, Daten Dritter u. a.) abzustimmen.

- Ebenfalls dem Grunde nach ist bei Berichtigung, Sperrung und Löschung von Daten die Benachrichtigung derjenigen Stellen vorzusehen, denen sie zuvor übermittelt wurden, soweit dem nicht ein unverhältnismäßiger Aufwand oder die geringe Sensibilität der Daten entgegenstehen.

Zu c):
Die Erhebung als Voraussetzung jeder weiteren Datenverarbeitung ist von ihrer Funktion her bereits einer der gravierendsten Eingriffe in das Recht auf informationelle Selbstbestimmung, zu dem sie auch im Volkszählungsurteil des Bundesverfassungsgerichts eindeutig gerechnet wird. Die Erhebung sollte daher im Landesdatenschutzgesetz und nicht an anderer Stelle geregelt werden. Ausnahmen vom Gebot der direkten Erhebung beim Betroffenen sind abschließend aufzuzählen, Erhebungen beim Betroffenen ohne dessen Kenntnis sollten nur aufgrund einer Rechtsvorschrift oder in bestimmten gravierenden Ausnahmefällen zulässig sein.

Zu d):
Die besondere Bedeutung, die das Bundesverfassungsgericht gerade der Zweckbindung bei der Verarbeitung personenbezogener Daten beimißt, erfordert ein grundsätzliches Verbot der Verarbeitung zu anderen Zwecken mit einer präzisen und abschließenden Aufzählung der aus überwiegenden Gründen des Allgemeinwohls gebotenen Ausnahmen. Dabei sind generalklauselartige Formulierungen zu vermeiden.

In diesem Zusammenhang ist auch zu prüfen, ob die Betroffenen dann benachrichtigt werden sollten, wenn aufgrund übergeordneten Rechts ihre personenbezogenen Daten in Bereiche übermittelt werden müssen, bei denen ein gleichwertiger Datenschutz nicht gesichert ist, wie z. B. an EG-Stellen oder internationale Organisationen.

Zu e):
Das Bundesverfassungsgericht weist in seinem Volkszählungsurteil der Kontrolle durch unabhängige Datenschutzbeauftragte eine tragende Funktion zu. Unbeschadet der bekannten Kritik der Datenschutzbeauftragten des Bundes und der Länder an den vorgesehenen Einschränkungen im Regierungsentwurf für ein BDSG ist die Stellung der Kontrollinstanz ihrer verfassungsrechtlichen Aufgabe entsprechend auszugestalten.

- So ist sicherzustellen, daß kein Bürger deshalb benachteiligt wird, weil er sich an den Datenschutzbeauftragten/Datenschutzkommission gewandt hat (Benachteiligungsverbot).

– Ebenso ist sicherzustellen, daß der DSB/DSK von allen Entwürfen für datenschutzrelevante Regelungen (Gesetze, Rechtsverordnungen und Verwaltungsvorschriften) rechtzeitig in Kenntnis gesetzt wird, und zwar auch dann, wenn diese Regelungen – von rein internen Vorüberlegungen abgesehen – Regelungen des Bundes oder der EG betreffen. Soweit diese Regelungen von Landesbehörden ausgeführt werden müssen, ist das Recht auf informationelle Selbstbestimmung der Bürger des Landes unmittelbar berührt.

– Ein Anhörungsrecht des DSB/DSK zu datenschutzrelevanten Entwürfen ist vorzusehen.

– In Entsprechung der Beratungspflicht gegenüber Landtag und Landesregierung sollte auch eine ausdrückliche Beratungspflicht des DSB/DSK gegenüber den kommunalen Spitzenverbänden sowie den Gewerkschaften und Personalvertretungen vorgesehen werden.

Zu f):
Die Neufassung der Regelung für den Bereich der Wissenschaft muß sich an einem vom Grundgesetz her vorgegebenen Spannungsverhältnis zwischen dem Recht auf informationelle Selbstbestimmung und dem in Artikel 5 garantierten Grundrecht auf Freiheit der Wissenschaft, Forschung und Lehre orientieren. In der Vergangenheit hat sich gezeigt, daß die bestehenden Bestimmungen in Kreisen der Wissenschaft vielfach als einengend empfunden werden. Mitunter wurden sie in ihrem Regelungsgehalt auch überinterpretiert. Dabei kann es vorkommen, daß Vorhaben von Wissenschaftlern ganz oder teilweise für unzulässig gehalten werden, obwohl bei näherer Prüfung doch noch eine befriedigende datenschutzrechtliche Lösung möglich wäre. Es muß vermieden werden, daß für die Allgemeinheit wichtige Forschungsvorhaben unterbleiben, eingeschränkt durchgeführt oder in das Ausland verlagert werden. Die zu treffende Regelung muß also in ihrer systematischen Struktur besonders klar und in ihrem Regelungsgehalt eindeutig sein.

Der schon an verschiedenen Stellen verwirklichte Rechtsgedanke, bestimmte Datenverarbeitungen für Forschungszwecke davon abhängig zu machen, ob das öffentliche Interesse an der Durchführung eines Forschungsvorhabens die schutzwürdigen Belange des Betroffenen (erheblich) überwiegt und der Zweck nicht auf andere Weise erreicht werden kann, sollte – soweit erforderlich – durchgängig angewendet werden. Dies muß auf jeden Fall nicht nur für die Übermittlung durch öffentliche Stellen, sondern auch für die Erhebung und ihre Form (Absehen von der schriftlichen Einwilligung) gelten.

Der Zeitpunkt der Trennung der Hilfsmerkmale und die Dauer ihrer Speicherung sind vom Forschungszweck abhängig zu machen. Hier ist zu prüfen, ob in allen Fällen auf den konkreten Forschungszweck abgestellt werden muß, oder ob es – zumindest in Ausnahmefällen – von der Bedeutung eines Forschungsbereichs für die Allgemeinheit her möglich sein sollte, Daten in bestimmtem Umfang auch für spätere, wahrscheinliche Forschungen zu speichern (Folgevorhaben). Sollte diesem Gedanken nähergetreten werden, müßte auf jeden Fall die Beteiligung einer unabhängigen Instanz vorgesehen werden (bestehend etwa aus Vertretern der Wissenschaft, der Öffentlichkeit und der unabhängigen Datenschutzkontrolle).

2.2.2 Automatisiertes Abrufverfahren

Automatisierte Abrufverfahren verursachen besondere Eingriffsrisiken. Ihre Einrichtung im Einzelfall muß daher der Zulassung durch spezielle Rechtsvorschrift vorbehalten bleiben. Die Landesregierung sollte zum Erlaß jeweils entsprechender Rechtsverordnungen ermächtigt werden. Dabei müssen Inhalt, Zweck und Ausmaß der erteilten Ermächtigungen im Gesetz bestimmt werden.

2.2.3 Berichtspflicht für den nichtöffentlichen Bereich

Um den Datenschutz im nichtöffentlichen Bereich stärker in das öffentliche Bewußtsein zu rücken und um Anregungen für einen verstärkten Erfahrungs- und Gedankenaustausch zu geben, sollte die Landesregierung verpflichtet werden, dem Landtag regelmäßig einen Bericht über die Tätigkeit der für den Datenschutz im nichtöffentlichen Bereich zuständigen Aufsichtsbehörden zu geben (vgl. Tz. 20.4).

2.2.4 Verhältnis zur Justiz

Nach § 24 Abs. 1 LDatG gelten die Bestimmungen des 4. Abschnitts (Überwachung des Datenschutzes) für Gerichte nur insoweit, als sie Aufgaben der Justizverwaltung wahrnehmen. Die Staatsanwaltschaften sind im Gesetzestext nicht genannt. Daraus ist zu folgern, daß insoweit die Bestimmungen des 4. Abschnitts ohne Einschränkung Anwendung finden. Dies sollte im Gesetz ausdrücklich bestimmt werden. Zu den hier bestehenden Streitpunkten mit der Justizverwaltung vgl. unten Tz. 7.3.2.

2.2.5 Abgrenzung zu den Aufgaben der Kommission des Landtags nach dem AG G 10

Eine ausdrückliche gesetzliche Abgrenzung der Zuständigkeiten der DSK hinsichtlich der Erhebung und Verarbeitung personenbezogener Daten, die der Kontrolle durch die G 10-Kommission unterliegen, besteht zur Zeit nicht. Eine klare und übersichtliche Regelung dieser Frage wäre nach Auffassung der DSK wünschenswert.

2.2.6 Behördliche Datenschutzbeauftragte

Jede datenverarbeitende Stelle sollte verpflichtet sein, einen behördeninternen Datenschutzbeauftragten zu bestellen, der die dafür erforderliche Sachkenntnis besitzt oder sich aneignet, und der nicht gleichzeitig mit Aufgaben der automatisierten Datenverarbeitung betraut sein darf. Um für kleine Stellen mit nur wenigen Bediensteten keine unverhältnismäßigen Belastungen entstehen zu lassen, sollte eine Sonderregelung getroffen werden. Der behördeninterne Datenschutzbeauftragte sollte das Recht erhalten, sich ohne Einhaltung des Dienstweges unmittelbar an den DSB/DSK zu wenden.

2.2.7 Medienprivileg

Das Recht auf informationelle Selbstbestimmung steht mit dem Grundrecht auf Rundfunkfreiheit in einem ähnlichen Kollisionsverhältnis wie mit dem Grundrecht auf Wissenschaftsfreiheit. Ebenso wie für die Datenverarbeitung zu Forschungszwekken muß für den Rundfunkbereich eine ausgewogene gesetzliche Konfliktlösung erarbeitet werden.
Die bloße Übernahme des derzeit geltenden Medienprivilegs mit mehr oder weniger unbedeutenden Rechten für die Betroffenen käme praktisch einer Beibehaltung der derzeitigen „Null-Lösung" gleich, die den Forderungen des Bundesverfassungsgerichts nicht gerecht würde.

Eine Regelung der Datenverarbeitung im publizistischen Bereich der öffentlich-rechtlichen Rundfunkanstalten sollte mindestens enthalten:

a) ein Auskunftsrecht, das dem Betroffenen dann zusteht, wenn er durch eine Berichterstattung in seinem Persönlichkeitsrecht betroffen wird. Die Auskunft sollte sich auf die der Berichterstattung zugrundeliegenden Daten zu seiner Person erstrecken. Inwieweit der Auskunftsanspruch zum Schutze sog. „Redaktionsgeheimnisse" (Namen der Verfasser von Beiträgen, von Einsendern und „Gewährsleuten") eingeschränkt werden kann, bedarf einer abwägenden Beurteilung. Mit dem Recht auf informationelle Selbstbestimmung unvereinbar wäre eine Aushöhlung des Anspruchs bis zu seiner praktischen Bedeutungslosigkeit,

b) das Recht des Betroffenen, bei Beeinträchtigung seines Persönlichkeitsrechts die Berichtigung oder Hinzufügung einer eigenen Darstellung von angemessenem Umfang zu verlangen,

c) eine Verpflichtung der Rundfunkanstalten, die gespeicherten Daten um Gegendarstellungen der Betroffenen zu ergänzen.

2.2.8 Fernmessen und Fernwirken (TEMEX)

Beim Betrieb von Fernmeß- und Fernwirkdiensten werden durch Datenverarbeitungs- oder Übertragungseinrichtungen bei Betroffenen, insbesondere in deren Wohnungen oder Geschäftsräumen, ferngesteuert Messungen vorgenommen oder andere Wirkungen ausgelöst. Die besondere Gefährdung des Rechts auf informationelle Selbstbestimmung wird in diesem Zusammenhang insbesondere darin gesehen, daß u. a. die Datenabrufe für die Betroffenen unbemerkt erfolgen und unbeeinflußt von ihnen erfolgen können. Soweit öffentliche Stellen des Landes die beschriebenen Möglichkeiten nutzen, sollten folgende Anforderungen gestellt werden:

a) Zur Verwirklichung der Zweckbindung dürfen die abgerufenen Daten nur für den dem Betroffenen angegebenen Zweck, wie z. B. Wasser- und Stromabrechnung, verwendet werden. Werden sie dafür nicht mehr benötigt, sind sie unverzüglich zu löschen.

b) Der Bürger sollte – abgesehen von einer ausdrücklichen gesetzlichen Regelung des Anschlusses – über seine Teilnahme frei entscheiden können.

c) Dazu ist er zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes der Dienste zu unterrichten (datenschutzrechtlicher Grundsatz der „informierten Einwilligung").

d) Dem Betroffenen dürfen keine Nachteile entstehen, wenn er sich weigert, teilzunehmen.

e) Eine einmal erteilte Einwilligung muß jederzeit widerrufen werden können, wenn dies mit der Zweckbestimmung des Dienstes vereinbar ist.

2.2.9 Kontrolle im Sicherheitsbereich

Der sog. Sicherheitsbereich ist nach dem Inkrafttreten bereichsspezifischer Normen (Polizeiverwaltungsgesetz und Landesverfassungsschutzgesetz), die auch das Recht auf Auskunft regeln, im wesentlichen noch durch die z. Z. in § 20 geregelte Unterstützungspflicht betroffen. Wie bei allen datenschutzrechtlichen Regelungen im Sicherheitsbereich ist auch hier zwischen dem Recht der Betroffenen einerseits und den sich unmittelbar aus den Grundrechten ergebenden staatlichen Schutzpflichten, hier dem Recht auf Sicherheit (Josef Isensee, „Das Grundrecht auf Sicherheit – zu den Schutzpflichten des freiheitlichen Verfassungsstaates", Walter de Gruyter-Verlag 1983), ein Spannungsverhältnis zu sehen, das besonders sorgfältige Abwägung erfordert.
Das Recht des Ministers des Innern, die Auskunft sowie die Einsicht in Unterlagen und Akten der Verfassungsschutzbehörde des Landes im Einzelfall zu verweigern, sollte nicht gegenüber dem DSB/DSK gelten. Um den berechtigten Interessen des Verfassungsschutzes an einem lückenlosen Quellenschutz Rechnung zu tragen, wären entsprechende Angaben von der Offenbarungspflicht auszunehmen. Ob weitere konkrete und eng umrissene Ausnahmen vorzusehen sind, ist zu prüfen.

Für die übrigen Stellen des Landes einschließlich der obersten Landesbehörden sollte es bei der bisherigen uneingeschränkten Auskunftspflicht verbleiben.

2.2.10 Dienst- und Arbeitsverhältnisse

Das informationelle Selbstbestimmungsrecht von Arbeitnehmern und Beamten sollte bereichsspezifisch geregelt werden. Schon jetzt sollten aber wesentliche datenschutzrechtliche Grundsätze für die Bediensteten öffentlicher Stellen im LDatG verankert werden. So ist die Verarbeitung ihrer personenbezogenen Daten strikt an das Erforderlichkeitsprinzip sowie an die sich aus Rechtsvorschriften, Tarifverträgen oder Dienstvereinbarungen ergebenden Notwendigkeiten zu binden. Weitere einschränkende Regelungen sind u. a. für die Datenübermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs, für die Auskunftserteilung, für die automatisierte Verarbeitung insbesondere von dienst- und arbeitsrechtlichen Beurteilungen sowie medizinischen und psychologischen Befunden zu treffen.

2.2.11 Einbeziehung neuer Informationstechniken

Dem technologischen Fortschritt auf dem Gebiete der Informations- und Kommunikationstechnik (z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) muß durch Einbeziehung von Regelungen in das LDatG Rechnung getragen werden.

3 Datenschutz auf europäischer Ebene

Auf europäischer Ebene besteht zur Zeit als einzige verbindliche datenschutzrechtliche Regelung die vom Ministerkommitee am 17. September 1980 genehmigte Europäische Datenschutzkonvention (Nr. 108), die bisher nur von einem Teil der 23 Staaten in Kraft gesetzt wurde. Auch die Bundesrepublik Deutschland hat die Konvention ratifiziert. Diese enthält außer verschiedenen zwischenstaatlichen Verfahrensregelungen eine Reihe materieller datenschutzrechtlicher Anforderungen für den Bereich der automatisierten Datenverarbeitung, so über die rechtmäßige Datenbeschaffung, die Festlegung von Zwecken der Datenverarbeitung einschließlich einer grundsätzlichen Zweckbindung, die Verpflichtung, gespeicherte Daten auf den neuesten Stand zu bringen sowie einen erhöhten Schutz für bestimmte als besonders sensibel eingestufte Datengruppen. Weitere Regelungen betreffen die Datensicherung und verschiedene Rechte der Betroffenen.

Daneben enthalten einige Artikel der Europäischen Menschenrechtskonvention vom 4. November 1950 Regelungen, aus denen sich unmittelbar datenschutzrechtliche Grundsätze herleiten lassen. Es sind dies der Schutz des Privat- und Familienlebens (Art. 8 EMRK), die Meinungs- und Informationsfreiheit (Art. 13) sowie die innerstaatliche Rechtsweggarantie (Art. 13). Fälle, die nach datenschutzrechtlichen Gesichtspunkten zu prüfen waren, sind in der Vergangenheit bereits von der Europäischen Kommission für Menschenrechte behandelt und vom Gerichtshof für Menschenrechte entschieden worden. Dabei ging es unter anderem um geheime Datenbeschaffung durch Telefonabhören, Briefkontrollen für Gefangene, die Weitergabe von Telefonabrechnungsdaten an die Polizei, Verarbeitung von Daten über das Privatleben durch die Polizei sowie über den Inhalt von Vormundschaftsakten (siehe hierzu Schweizer, „Europäisches Datenschutzrecht – was zu tun bleibt", DUD Heft 11 vom November 1989, S. 542 ff).

In den 12 Mitgliedsstaaten der Europäischen Gemeinschaft ist der Datenschutz sehr unterschiedlich geregelt. Während in Frankreich und in der Bundesrepublik Deutschland der Datenschutz umfassend und detailliert normiert ist, gibt es einige Staaten, die über kein umfassendes Datenschutzrecht verfügen. Besonders bemerkenswert ist das Fehlen eines institutionalisierten Datenschutzes bei der EG, die mit Normen unterschiedlicher Wirksamkeit Datenverarbeitungen der verschiedensten Art vorschreibt. Es exisiert bei der EG weder eine allgemeine datenschutzrechtliche Regelung noch eine Instanz, um die Einhaltung wenigstens der wichtigsten datenschutzrechtlichen Grundsätze zu überwachen. Eine gleichwie geartete Anwendung der Europaratskonvention ist in der Praxis der EG-Kommission nicht festzustellen. Dennoch bedienen sich Einrichtungen der EG in zunehmendem Maße Datenbanken, die auch personenbezogene Daten führen.

Probleme durch Datenschutzdefizite in erheblichem Ausmaß sind nicht nur bei der Verwirklichung des bevorstehenden EG-Binnenmarktes zu erwarten, wenn Kreditinformationen, Adressen, Kundendaten u. a. EG-weit ausgetauscht oder gar in sogenannten „Daten-Paradies-Ländern" schutz- und kontrollfrei verarbeitet werden können. Auch im öffentlich-rechtlichen Bereich führt die unterschiedliche Datenschutzrechtslage zwangsläufig zu Schwierigkeiten, wie es sich gerade im Sicherheitsbereich bei der Durchführung des im Zusammenhang mit dem Abbau von Grenzkontrollen geschaffenen „Schengener Übereinkommens" zeigt.

Für Personen, deren Rechte durch die umfassende allgemeine und bereichsspezifische Datenschutzgesetzgebung in der Bundesrepublik Deutschland geschützt sind, zeichnet sich durch die faktische Entwicklung in der EG die Gefahr massiver Rechtsbeeinträchtigung ab.

Die durch die geschilderte Situation aufgeworfenen Fragen waren Gegenstand der 11. Internationalen Konferenz der Datenschutzbeauftragten.

Die Konferenz verabschiedete zwei Resolutionen über die Bedeutung des Datenschutzes für den internationalen Datenverkehr. In der „Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten" vom 30. August 1989 wird insbesondere auf die bereits genannte Konvention Nr. 108 des Europarates hingewiesen und bedauert, daß ihr bislang nicht alle Staaten beigetreten sind. In einer Zusatzerklärung der Datenschutzbeauftragten der EG-Länder werden die Europäische Gemeinschaft und ihre Mitgliedsstaaten aufgefordert, in ihre Planungen für „Europa 92" die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen. Im einzelnen wird vorgeschlagen, die Grundsätze der Konvention Nr. 108 für alle Mitgliedsstaaten sowie für die Institutionen der EG selbst verbindlich vorzuschreiben und zur Überwachung eine unabhängige Datenschutzkontrollinstanz einzurichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der DSK hat sich auf ihrer Tagung vom 26./27. Oktober 1989 in einer Entschließung den Forderungen der Datenschutzbeauftragten der EG-Länder im wesentlichen angeschlossen und dabei einmütig gefordert, daß bei der Entwicklung und Nutzung grenzüberschreitender Datennetze und Datendienste dem Datenschutz der gleiche Stellenwert zukommen muß, wie der Förderung der technischen Infrastruktur (vgl. Anlage 1).

Die DSK bedauert, daß durch die Untätigkeit der EG-Kommission auf diesem Gebiet die technische Entwicklung im europäischen Bereich der notwendigen Grundrechtssicherung davonläuft. Es kann nicht angehen, daß auf dem wichtigen Gebiet der Sicherung von Menschenrechten nicht einmal der Standard durch die EG-Kommission gesichert wird, der an anderer Stelle auf europäischer Ebene bereits anerkannt ist.

4 Meldewesen

4.1 Archivierung und Löschung von Meldedaten

Nach § 11 Abs. 3 Meldegesetz (MG) sind nach Ablauf von fünf Jahren nach dem Ende des Jahres des Wegzugs oder des Todes eines Betroffenen die in § 3 Abs. 1 Nr. 1 – 7 und 10 – 19 sowie Abs. 2 Nr. 9 MG genannten Daten für die Dauer von 50 Jahren gesondert aufzubewahren und durch technische und organisatorische Maßnahmen besonders zu sichern. Während dieser Zeit dürfen sie nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der in § 31 Abs. 3 MG genannten Behörden oder für Wahl- oder Abstimmungszwecke unerläßlich ist oder der Betroffene vorher schriftlich zugestimmt hat. § 11 Abs. 4 MG ermächtigt den Minister des Innern und für Sport, durch Rechtsverordnung das Nähere über das Verfahren der Löschung, der gesonderten Aufbewahrung und die erforderlichen Sicherungsmaßnahmen zu bestimmen.

Im Zusammenhang mit der Archivierung von Meldedaten stellte die DSK folgendes fest:

Entgegen dem Wortlaut des § 11 Abs. 3 MG („nach Ablauf von fünf Jahren") erfolgt die Archivierung der Meldedaten unmittelbar nach dem Tod oder dem Wegzug eines Bürgers, indem die Daten in eine Archivdatei eingestellt werden.

Trotz dieser Archivierung können alle rheinland-pfälzischen Meldebehörden auf die Archivdaten im gleichen Maß wie auf aktuelle Daten zugreifen. Besondere technische und organisatorische Sicherungsmaßnahmen wurden hinsichtlich der Archivdaten nicht getroffen.

Die DSK forderte das ISM auf zu veranlassen, daß die besonderen technischen und organisatorischen Sicherungsmaßnahmen durch das Landesrechenzentrum vorgenommen werden. Schließlich erhob die DSK gegenüber dem ISM die Forderung, darauf hinzuwirken, daß die länger als fünf Jahre gespeicherten Archivdaten grundsätzlich nicht mehr genutzt werden (§ 11 Abs. 3 Nr. 2 MG).

Eine Überprüfung der archivierten Daten hatte im übrigen ergeben, daß die Löschungsregelung des § 11 MG nach Ablauf der 5-Jahresfrist nicht beachtet wird.

Die DSK forderte die strenge Beachtung der Löschungsbestimmungen des MG. Soweit Speicherungen generell unzulässig sind, muß die Löschung nicht nur in den archivierten, sondern auch in den aktuellen Datensätzen durchgeführt werden.

Schließlich wurde von der DSK angesichts der festgestellten Probleme empfohlen, die nach § 11 Abs. 4 MG mögliche „Rechtsverordnung über das Verfahren der Löschung, der gesonderten Aufbewahrung und die erforderlichen Sicherungsmaßnahmen" zu erlassen.

4.2 Datenübermittlung an kommunale Gebietsrechenzentren zur Erledigung kommunaler Aufgaben

Nach § 2 MG haben die Meldebehörden die in ihrem Zuständigkeitsbereich wohnhaften Einwohner zu registrieren, um deren Identität und Wohnungen feststellen und nachweisen zu können. Zur Erfüllung dieser Aufgaben führen sie Melderegister.

Im Grundsatz ist das Melderegister also ein Auskunftsinstrument. Nicht nur Behörden und andere Stellen des öffentlichen Bereichs, sondern auch Privatpersonen, Firmen usw. können beim Meldeamt Informationen nachfragen, die sie für die Erfüllung ihrer Aufgaben oder für die Verfolgung von Rechtsansprüchen benötigen. Die Voraussetzungen einer Auskunftserteilung aus dem Melderegister wurden vom Gesetzgeber unter Berücksichtigung des Erforderlichkeitsprinzips so differenziert bestimmt, wie dies unter verfassungsrechtlichen Gesichtspunkten geboten ist.

Ergänzt werden die gesetzlichen Übermittlungs- und Auskunftsbestimmungen durch Vorschriften über die Berücksichtigung von Auskunftssperren, die zu einer von der allgemeinen Regelung abweichenden Verfahrensweise im Einzelfall führen. Solche Auskunftssperren werden in der Regel von den Betroffenen beantragt; nur die Auskunftssperre wegen einer Gefahr für Leib und Leben nach § 34 Abs. 5 ist auch von Amts wegen einzutragen.

Die Nichtberücksichtigung einer solchen Auskunftssperre, die eine geschiedene Frau wegen ständiger Bedrohungen durch ihren früheren Ehemann nach einem Wohnungswechsel in das Melderegister eintragen ließ, führte vor einigen Jahren zu Schadensersatzleistungen einer Gemeinde über mehrere tausend DM.

Bisweilen ist die Auskunftssperre selbst ein recht empfindliches Datum. Wird sie beispielsweise zum Schutze der Identität eines adoptierten Kindes eingetragen, so kann bereits die Übermittlung der Tatsache, daß eine Auskunftssperre aus diesem Grunde besteht, schutzwürdige Belange beeinträchtigen. Das Bestreben der zuständigen Meldebehörden muß also dahin gehen, auch Auskunftssperren nur in dem erforderlichen Umfange zu übermitteln.

Im Berichtszeitraum war konkret die Frage zu beurteilen, ob es zulässig ist, in die regelmäßige Datenübermittlung an Städte und Gemeinden nach § 31 Abs. 7 MG – sog. Kommunaler Austauschdatensatz (KADS) – auch Auskunftssperren einzubeziehen. Die Städte und Gemeinden waren der Auffassung, die Einbeziehung der Auskunftssperren in den KADS beanspruchen und unter Verwendung dieses Datensatzes melderechtliche Aufgaben – wie z. B. die Datenübermittlung an Adreßbuchverlage – erfüllen zu können. Die DSK nahm zu dieser Frage wie folgt Stellung:

Rechtsgrundlage für die Beurteilung der Verfahrensfrage ist § 37 Abs. 1 MG. Danach sollen die Meldebehörden ihre Aufgaben mit Hilfe des beim Landesrechenzentrum betriebenen und unterhaltenen landeseinheitlichen Verfahrens für das Meldewesen erfüllen. Demzufolge dürfen zur Erfüllung von Aufgaben der Meldebehörden nur Daten verwendet werden, die dem beim Landesrechenzentrum geführten Datenbestand unmittelbar entnommen sind.

Auskunftssperren dürfen in den kommunalen Austauschdatensatz nur einbezogen werden, wenn ihre Kenntnis zur Erfüllung von Aufgaben der empfangenden Stelle erforderlich ist. Da die Übermittlung von Meldedaten an Adreßbuchverlage eine Auf-

gabe ist, die von den Meldebehörden unter Verwendung der beim Landesrechenzentrum gespeicherten Meldedaten wahrzunehmen ist, wäre eine Übermittlung entsprechender Auskunftssperren (§ 35 Abs. 4 MG) im Rahmen des KADS zum Zweck einer Nutzung durch andere Stellen der Verwaltung unzulässig.

4.3 Zugriff auf EWOIS-Daten durch Kfz-Zulassungsstellen

Die räumliche Begrenzung des Zuständigkeitsbereichs von Behörden ist unter Datenschutzgesichtspunkten von großer Bedeutung. Sie bildet einen Teilaspekt der sog. „Informationellen Gewaltenteilung". Nur in Ausnahmefällen sollen Behörden über die Daten von Bürgern verfügen können, die nicht in ihrem Zuständigkeitsbereich wohnen. Ein Problem besteht darin, daß die zentrale Datenbankverwaltung die technischen Voraussetzungen für einen erleichterten Zugriff auf Meldedaten bietet und deshalb solche Zugriffsmöglichkeiten nach großzügiger Auslegung des Erforderlichkeitsprinzips auch genutzt werden.

Im Berichtszeitraum wurde beispielsweise festgestellt, daß die Kfz-Zulassungsstellen auf die in § 5 MeldDÜVO aufgeführten Daten aller rheinland-pfälzischer Einwohner und nicht nur auf die Daten ihres Zuständigkeitsbereichs zugreifen können. Die DSK vertrat gegenüber dem ISM die Auffassung, daß dieser umfassende Zugriff nicht erforderlich ist. Eine derartige Zugriffsmöglichkeit müsse als unverhältnismäßig bezeichnet werden. Auch dann, wenn ein Fahrzeughalter seiner Pflicht nicht nachkomme und einen Wohnungswechsel der Zulassungsstelle nicht mitteile, könne durch eine Rückfrage beim zuletzt zuständigen Meldeamt festgestellt werden, wie die aktuelle Anschrift laute. Hinzu komme, daß nur ein verschwindend geringer Bruchteil der im EWOIS gespeicherten Datensätze in der Praxis tatsächlich aufgrund eines überregionalen Zugriffs benötigt werde. Demgegenüber seien aber alle im EWOIS gespeicherten Daten mit der Einrichtung eines Online-Zugriffs als übermittelt anzusehen (§ 3 Abs. 2 Nr. 2 LDatG).

Unter Berücksichtigung dieser Gesichtspunkte kam die DSK zu dem Ergebnis, daß die Kfz-Zulassungsstellen im Online-Verfahren nur auf diejenigen EWOIS-Daten zugreifen dürfen, die Personen zuzuordnen sind, die ihren Wohnsitz im Zuständigkeitsbereich der jeweiligen Zulassungsstelle haben.

Eine abschließende Stellungnahme des ISM hierzu liegt noch nicht vor. Die Angelegenheit wird von der DSK weiter verfolgt.

4.4 Übermittlung personenbezogener Daten von Kindern, die in einem Adoptionspflegeverhältnis stehen

Mehrfach hatte sich die DSK im Berichtszeitraum mit der Übermittlung von Meldedaten von Kindern, die in einem Adoptionspflegeverhältnis (§ 1744 BGB) stehen, an öffentlich-rechtliche Religionsgesellschaften zu befassen. Die Daten wurden weitergegeben, obwohl die Datensätze der Kinder mit einem entsprechenden Sperrvermerk versehen waren. Die DSK kam nach Prüfung der Rechtslage zu dem Ergebnis, daß die Übermittlung der Meldedaten von Kindern in einem Adoptionspflegeverhältnis an Religionsgesellschaften unzulässig ist. Grundsätzlich dürfen zwar den öffentlich-rechtlichen Religionsgesellschaften Meldedaten nach Maßgabe von § 32 MG übermittelt werden. Bei Kindern, die in einem Adoptionspflegeverhältnis stehen, ist jedoch ergänzend zu dieser Vorschrift § 1758 Abs. 2 i. V. mit Abs. 1 BGB zu beachten, wonach Tatsachen, die geeignet sind, die beabsichtigte Annahme und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden nicht offenbart werden dürfen, es sei denn, daß besondere Gründe des öffentlichen Interesses dies erfordern. Die Notwendigkeit einer besonderen Betreuung, auf die das Landesrechenzentrum hinwies, steht nach Auffassung der DSK außer Verhältnis zur Gefährdung des Adoptionsgeheimnisses, die mit der Datenübermittlung einhergeht. Wenn eine solche Notwendigkeit besteht, kann ihr im übrigen am besten durch Übermittlung der Anschrift der Adoptionspflegeeltern entsprochen werden, denn sie und nicht – wie im konkreten Fall – ein Kleinkind kämen als Adressaten von Schreiben mit Betreuungsangeboten in Betracht. Die Übermittlung des noch nicht geänderten Familiennamens eines Kindes mit seiner der Anschrift des Annehmenden entsprechenden Wohnanschrift ist geeignet, die Tatsache der beabsichtigten Annahme und die Herkunft des Kindes zu offenbaren. Auch die Meldebehörden sind Adressaten des § 1758 BGB. Besondere Gründe des öffentlichen Interesses, die eine Offenbarung rechtfertigen könnten, waren für die DSK nicht erkennbar.

Die DSK bat das ISM, das LRZ anzuweisen, in Fällen der geschilderten Art die Meldedatenübermittlung einzustellen. Das ISM hat jedoch der Auffassung der DSK zunächst widersprochen. Nach Einholung einer Stellungnahme der betroffenen Religionsgesellschaften wird vom ISM abschließend über die Frage der Übermittlung der Daten von Adoptionspflegekindern entschieden werden.

4.5 Melderegisterauskünfte an politische Parteien

Eine Verbandsgemeindeverwaltung fragte bei der DSK an, ob es zulässig sei, daß der rechtsradikalen Partei „Deutsche Volksunion – Liste D" (DVU) Meldedaten von Wählern gem. § 35 MG überlassen werden. Die DSK wies darauf hin, daß die Meldebehörde einer Partei nach § 35 Abs. 1 MG im Zusammenhang mit Wahlen eine einfache Melderegisterauskunft (§ 34 Abs. 1 MG) über Wahlberechtigte erteilen darf, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Nach dieser Vorschrift hat der Antragssteller (die Partei) einen Anspruch auf fehlerfreie Ermessensausübung, der sich bei ständiger

gleichmäßiger Verwaltungspraxis unter dem Gesichtspunkt der Selbstbindung der Verwaltung als Ausfluß des Gleichbehandlungsgrundsatzes zu einem Rechtsanspruch verdichten kann. Dies bedeutet, daß auch der „Deutschen Volksunion" dann Auskunft zu erteilen ist, wenn anderen Parteien eine entsprechende Auskunft erteilt wurde bzw. bei Anfrage erteilt würde und wenn keine – etwa aus der spezifischen Programmatik der DVU herzuleitenden – wesentlichen Gründe für eine Ungleichbehandlung bestehen. Die in diesem Zusammenhang zu treffende Wertung stellt jedoch keine datenschutzrechtliche Frage dar, so daß die DSK dazu keine Stellung nehmen konnte.

Zu einem späteren Zeitpunkt mußte von der DSK festgestellt werden, daß die der DVU von den Meldebehörden übermittelten Meldedaten nicht nur zu Wahlwerbungszwecken verwendet wurden. Beispielsweise wurden von der DVU angeschriebene Bürger auch aufgefordert, bestimmte Wochenzeitungen zu abonnieren oder der DVU bzw. nahestehenden Organisationen beizutreten.

Hinsichtlich der Mitgliederwerbung sowie der Werbung zum Bezug von Wochenzeitungen vertritt die DSK die Auffassung, daß diese Datenverwendung außerhalb der Zweckbestimmung des § 35 MG liegt. Die unzulässige Verwendung der Daten könnte von den Meldebehörden als Ordnungswidrigkeit verfolgt werden.

5 Polizei

5.1 Vorbemerkung

Während des Berichtszeitraums hat sich der Einsatz der automatisierten Datenverarbeitung auch im Polizeibereich weiterentwickelt, wobei hier ebenfalls eine zunehmende Tendenz zum Einsatz dezentraler Systeme besteht. Dies zeigt sich im vermehrten PC–Einsatz auch bei kleineren Polizeidienststellen, insbesondere im repressiven Bereich. Nachdem beim ISM zunächst die Meinung vorherrschte, daß aufgrund bestehender Sicherheitsdefizite auf den Einsatz von PC im Polizeibereich grundsätzlich verzichtet werden sollte, hat sich mittlerweile für die Polizei doch aufgrund von Rationalisierungszwängen die Notwendigkeit ergeben, PC einzusetzen. Durch den beabsichtigten Einsatz von Sicherungssoftware sollen allerdings die Sicherheitsrisiken vermindert werden.

Als Beispiel für die Entwicklung zu dezentralen Systemen kann auf POLADIS (vgl. Tz. 5.2.1) hingewiesen werden.

Von einer neuen Qualität der Datenverarbeitung ist die internationale Zusammenarbeit der Polizei. Hier soll das Schengener Informationssystemen (SIS) dazu dienen, durch den Grenzabbau („EG 92") entstehende Sicherheitsdefizite auszugleichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der DSK Rheinland-Pfalz vom 26./27. Oktober 1989 hat wegen der mit der Installation eines solchen Systems verbundenen Gefahrenpotentiale eine Entschließung darüber verabschiedet (vgl. Anlage 2), was aus datenschutzrechtlicher Sicht bei der Verwirklichung dieses grenzüberschreitenden Systems beachtet werden muß.

Die Schwerpunkte der Überprüfungstätigkeit der DSK während des Berichtszeitraumes lassen sich den folgenden Ausführungen entnehmen.

5.2 Neue Dateien

5.2.1 POLADIS

Bei der Kreisverwaltung des Donnersbergkreises (Kirchheimbolanden) und beim Polizeipräsidium Mainz wurde im Rahmen eines Pilotprojekts das „Polizeiliche Anwenderorientierte Dezentrale Informations-System (POLADIS)" eingeführt.

Das System POLADIS besteht aus der automatisierten Vorgangsverwaltung (AVV-POL), der automatisierten Verkehrsunfallsachbearbeitung (ASB-VU) sowie der automatisierten Strafanzeigensachbearbeitung (ASB-ST). Anlaß für die Einrichtung dieser Dateien war die Registrierung und Dokumentation der polizeilichen Vorgänge in unterschiedlichen Tagebüchern. Die Fülle der diversen Aktenerschließungskriterien führt dazu, daß für jeden polizeilichen Vorgang eine Vielzahl von Eintragungen in verschiedene Bücher vorgenommen werden muß. Der zeitliche Aufwand für die Erfassungen sowie der für das Auffinden eines Vorganges erforderliche Suchaufwand gehen zu Lasten der eigentlichen polizeilichen Arbeit.

Die Datei AVV-POL stellt ein elektronisches Verfahren zur Registrierung, Verwaltung und Dokumentation aller polizeilichen Vorgänge einer Dienststelle dar.

Bei der Datei ASB-VU handelt es sich um ein elektronisches Verfahren für die Automatisierung des Formularwesens, zur Unterstützung der Melde- und Berichtspflichten sowie zur Automatisierung der Statistiken bei Verkehrsunfällen.

Das Verfahren ASB-ST dient der Automatisierung des Formularwesens, der Unterstützung der Melde- und Berichtspflichten sowie der Automatisierung der Statistiken bei Strafanzeigen.

Nach Auffassung der DSK muß bei diesen Verfahren berücksichtigt werden, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in das Datenverarbeitungssystem eingegeben wurden (§ 1 Nr. 7 der Landesverordnung zu § 9 LDatG). Dies bedeutet, daß bei der Eingabe von Daten in zentrale Systeme (POLIS) über Anlagen des dezentralen Informationssystems eine Protokollierung erfolgen muß, wer von welchem Bildschirm des dezentralen Informationssystems die Eingabe vorgenommen hat. Zumindest im dezentralen Informationssystem muß eine solche Protokollierung durchgeführt werden. Auch für Zugriffe auf Daten zentraler Informationssysteme über das System POLADIS sollte nach Auffassung der DSK eine entsprechende Protokollierung eingeführt werden. Schließlich sollte programmäßig vorgesehen werden, daß gespeicherte Dokumente grundsätzlich nachträglich nicht mehr geändert werden können, sondern daß immer dann, wenn eine Änderung erforderlich wird, ein neues Dokument angelegt werden muß. Der für die Sachbearbeiter relevante Akteninhalt soll nach Auffassung der DSK mit den vorhandenen Speicherungen übereinstimmen, damit dann, wenn zur Bearbeitung des Vorgangs nur auf die automatisierten Verfahren zurückgegriffen wird, durch das Fehlen gespeicherter Dokumente keine falschen Schlüsse durch die die Angelegenheit bearbeitenden Polizeibeamten gezogen werden. Zwischen der DSK und dem ISM werden über diese Forderungen zur Zeit Gespräche geführt.

5.2.2 Arbeitsdatei „MENZU" (Menschenhandel und Zuhälterei)

Vom ISM wurde die Arbeitsdatei „MENZU" angemeldet. Grund für die Errichtung dieser Datei war die Erkenntnis, daß in Fällen des Menschenhandels, der Förderung der Prostitution und der Zuhälterei strafbares Verhalten oft nur schwer erkennbar und nachweisbar ist. Die Ermittlungen erstrecken sich häufig auf einen mehrjährigen Zeitraum. Darüber hinaus werden Prostituierte von Zuhältern und deren Gehilfen häufig an andere Orte verbracht, sobald bekannt wird, daß polizeiliche Ermittlungen geführt werden. Frauen, die zur Prostitution gebracht werden, wechseln die von Zuhältern unterhaltenen Etablissements und werden in Zuhälterkreisen ausgetauscht.

Zur Bekämpfung dieser Kriminalität war nach Auffassung der rheinland-pfälzischen Polizei die Errichtung der Datei „MENZU" erforderlich. Sie soll die Erkenntnisse verschiedener Polizeidienststellen aus dem Bereich Prostitution und Zuhälterei zusammenführen und eine landesweite Auswertung ermöglichen. Auf diese Weise sollen örtlich und zeitlich auseinanderliegende Zusammenhänge dennoch erkennbar gemacht werden.

Die Eingabe der Daten erfolgt zentral beim LKA und bei den fünf Polizeipräsidien des Landes. Abfrageberechtigt sind die zuständigen Beamten des Landeskriminalamtes sowie der fünf Polizeipräsidien.

Bei einer Überprüfung der Datei in einem rheinland-pfälzischen Polizeipräsidium konnte festgestellt werden, daß keine allgemeine Prostituiertendatei aufgebaut wird. In die Datei werden lediglich personenbezogene Daten solcher Personen eingestellt, die im Verdacht stehen, Straftaten gegen die sexuelle Selbstbestimmung zu begehen. Auch die Daten von (ggf. in Barbetrieben beschäftigten) Prostituierten werden gespeichert, wenn diese als mögliche Zeugen in Frage kommen. Sie werden dann als sog. „andere Personen" in der Datei ausdrücklich gekennzeichnet. Nach Auffassung der DSK bestehen gegen diese Speicherungen keine Bedenken. Im Rahmen der Überprüfung konnte festgestellt werden, daß keine sensiblen Daten wie beispielsweise die Erkrankung an AIDS gespeichert werden. Sobald die Speicherung personenbezogener Daten nicht mehr erforderlich ist, werden diese gelöscht.

5.2.3 Schiffbewegungsdatei

Vom ISM wurde die DSK über die Absicht unterrichtet, eine sog. „Schiffskontrolldatei" in automatisierter Form einzurichten. Diese sei zur Wahrnehmung schiffahrtspolizeilicher Vollzugsaufgaben durch die Wasserschutzpolizei erforderlich, um den Schiffsverkehr auf den Bundeswasserstraßen zu kontrollieren. Dabei sollen Mängel an Schiffen festgestellt werden, die eine Gefahr für die Sicherheit und Leichtigkeit des Schiffsverkehrs oder schädliche Umwelteinwirkungen verursachen können. Schließlich sollen mit Hilfe dieser Datei behindernde und Kosten verursachende Mehrfachkontrollen eines Schiffes durch die Wasserschutzpolizei vermieden werden. Zum anderen muß, so das ISM, angesichts der hohen Verkehrsfrequenz auf den Bundeswasserstraßen und der zunehmenden Unfallgefahr die Effektivität der Kontrolltätigkeit der Wasserschutzpolizei verbessert werden.

Folgende Daten sollen in dieser Datei gespeichert werden:

Schiffsname, Schiffsnummer, Schiffsgattung, Kontrollort, Kontrolldatum, Kontrollzeit, Stromkilometer, Fahrtrichtung, Reiseziel, Gefahrgutklassifizierung, festgestellte Mängel, Bilgeninhalt, sowie von der Polizei veranlaßte Maßnahmen. Dabei handelt es sich um personenbeziehbare Daten.

Abfrageberechtigt sollen die Beamten und Angestellten der Dienststellen der Wasserschutzpolizei Rheinland-Pfalz sein, die mit der Kontrolle von Schiffen befaßt sind.

Eine bereichsspezifische Rechtsgrundlage im Binnenschiffahrtsaufgabengesetz (BinSchAufgG) vom 4. August 1986 (BGBl. I S. 1270) für die Speicherung personenbezogener Daten zur Durchführung schiffahrtspolizeilicher Aufgaben besteht nicht. Nach Auffassung der DSK kann die Datei nach § 25 a Abs. 1 Ziff. 1 PVG als zulässig angesehen werden. Die DSK würde es jedoch im Interesse einer völlig zweifelsfreien Rechtsgrundlage begrüßen, wenn mittelfristig bereichsspezifische Regelungen über die Erhebung und Verarbeitung personenbezogener Daten in das Gesetz über die Aufgaben des Bundes auf dem Gebiet der Binnenschiffahrt aufgenommen würden.

Für den nächsten Berichtszeitraum ist eine Überprüfung der in der Datei konkret gespeicherten Einzelfälle beabsichtigt.

5.3 Polizeiliche Meldedienste

5.3.1 Meldedienst wichtige Ereignisse (WE-Meldungen)

Aufgrund einer Anregung der DSK wurde vom ISM im Berichtszeitraum der „Meldedienst wichtige Ereignisse" überarbeitet.

Hierbei handelt es sich um Richtlinien, aus denen sich ergibt, wann bei „wichtigen Ereignissen" vorgesetzte Dienststellen zu unterrichten sind. In den Richtlinien wird im einzelnen dargelegt, bei welchen Vorkommnissen es sich um „wichtige Ereignisse" handelt. Anlaß für die DSK, sich mit diesem Meldedienst zu befassen, war die Eingabe eines Bundeswehrangehörigen, der sich darüber beschwerte, daß zahlreiche zivile und militärische Dienststellen von einer Polizeidienststelle darüber informiert wurden, daß er eine Trunkenheitsfahrt unternommen hatte.

Nicht zulässig war nach Auffassung der DSK die Unterrichtung des MAD, eines nahegelegenen Polizeipräsidiums sowie eines Korps der Bundeswehr.

Aufgrund der im Zusammenhang mit der Eingabe durchgeführten Überprüfung der Richtlinien ergaben sich Zweifel, ob bei allen dort angesprochenen zu meldenden Sachverhalten eine polizeiliche Zuständigkeit besteht. Ergänzend sollte nach Auffassung der DSK geklärt werden, ob die Festlegungen im „Meldedienst" mit den später in Kraft getretenen §§ 25 a ff PVG in Einklang stehen.

Das ISM griff diese Anregung der DSK auf und legte neue Richtlinien über die Meldung wichtiger Ereignisse vor.

Ziffer 2.3 dieser neuen Richtlinien lautete nunmehr: „Zu melden sind bedeutsame Ereignisse, bei denen Personen der Zeitgeschichte oder Angehörige der stationierten Streitkräfte beteiligt sind." Die DSK äußerte gegenüber dem ISM, daß diese Formulierung zumindest mißverständlich sei und schlug folgende Fassung vor: „Besonders bedeutsame Vorkommnisse im Zusammenhang mit Versammlungen und sonstigen Veranstaltungen, soweit polizeiliches Einschreiten erforderlich wurde." Zu Satz 2 wurde dem ISM folgender Vorschlag der DSK unterbreitet: „Zu melden sind auch bedeutsame Ereignisse, die polizeiliche Maßnahmen erforderten und bei denen Personen der Zeitgeschichte oder Angehörige der Stationierungsstreitkräfte beteiligt waren."

Das ISM teilte mit Schreiben vom 19. Juni 1989 der DSK mit, daß diese Formulierungsvorschläge Zustimmung fänden. Bei der nächsten Änderung sollen sie berücksichtigt werden.

Im übrigen waren von der DSK keine Bedenken aus datenschutzrechtlicher Sicht gegen die neuen Richtlinien zu erheben. Sie stehen in Übereinstimmung mit den im PVG enthaltenen Übermittlungsvorschriften.

5.3.2 Meldedienst „Landfriedensbruch und verwandte Straftaten"

Auch die rheinland-pfälzische Polizei beteiligt sich an dem kriminalpolizeilichen Meldedienst „Landfriedensbruch und verwandte Straftaten". Ziel des Meldedienstes ist es durch die zentrale Sammlung und Auswertung von Erkenntnissen überregional oder steuernd handelnde Straftäter oder Tatzusammenhänge zu erkennen und dadurch Hinweise für die Verhütung von Straftaten im Zusammenhang mit öffentlichen Versammlungen oder Aufzügen zu erhalten. Nach diesen Richtlinien haben die Polizeidienststellen dem BKA über das jeweilige LKA die Einleitung entsprechender Ermittlungsverfahren unter Angabe der Personalien des Beschuldigten zu melden. Diese Daten werden beim BKA in eine Zentraldatei (APLF) eingestellt. Zur Verhütung von Straftaten im Zusammenhang mit Demonstrationen werden aus aktuellem Anlaß auf Anforderung der für den Einsatz zuständigen Polizeidienststelle bestimmte gespeicherte Personen- und Kfz-Daten zur Abfrage im Inpol-Fahndungsbestand bereitgehalten.

Einem Erfahrungsbericht über den Betrieb dieser Datei war zu entnehmen, daß von rheinland-pfälzischen Polizeidienststellen die Daten von 109 Personen zur Speicherung in der Datei APLF dem BKA gemeldet waren. Im Rahmen einer Überprüfung konnte festgestellt werden, daß nur noch 25 Personendatensätze gespeichert waren. Die Namen dieser 25 Personen wurden der DSK mitgeteilt. Sie wurden anläßlich gewalttätiger demonstrativer Aktionen vor dem Atomkraftwerk Mülheim-Kärlich für die Kreisverwaltung Mayen-Koblenz gespeichert.

Eine bei dem zuständigen Kriminalkommissariat durchgeführte Überprüfung ergab, daß gegen diese Personen Ermittlungsverfahren wegen des Verdachts einer Straftat nach § 125 StGB (Landfriedensbruch) eingeleitet worden waren.

Den Betroffenen konnten jedoch keine konkreten Gewalthandlungen nachgewiesen werden, so daß alle Verfahren nach § 170 Abs. 2 StPO eingestellt wurden. Gespeichert wurden diese Personen in der Datei APLF für eine Dauer von drei Jahren. Nach Beendigung der Überprüfung bei dem zuständigen Kriminalkommissariat wurden alle 25 Personendatensätze in der Datei APLF gelöscht. Zu diesem Zeitpunkt waren damit in APLF keine von rheinland-pfälzischen Polizeidienststellen veranlaßte Speicherungen vorhanden.

5.4 Datenübermittlungen

5.4.1 Übermittlung personenbezogener Daten durch die Polizei an den sozialpsychiatrischen Dienst der Gesundheitsämter bei Selbstmordversuchen

Zukünftig werden die Daten von Personen, die einen Selbstmordversuch unternommen haben, grundsätzlich nur noch mit ihrer Einwilligung an den sozialpsychiatrischen Dienst der staatlichen Gesundheitsämter übermittelt. Dies war das Ergebnis von Gesprächen, die die DSK mit Vertretern des ISM und des MUG geführt hat.

Anlaß für diese Gespräche waren der DSK vorliegende Informationen, wonach bei Selbstmordversuchen auch dann, wenn die Betroffenen bereits zu Behandlungszwecken stationär in ein Krankenhaus eingeliefert worden waren, die Polizei jeweils das zuständige Gesundheitsamt informiert hat. Zukünftig werden die behandelnden Ärzte die Betroffenen in einem Beratungsgespräch auf die Hilfsmöglichkeiten durch die Gesundheitsämter hinweisen.

Zu einem solchen Hinweis auf Hilfsmöglichkeiten sollen auch die Polizeibeamten verpflichtet werden. Dazu wird vom MUG ein Merkblatt entworfen und den Betroffenen von der Polizei ausgehändigt. Soweit dann eine Übermittlung personenbezogener Daten durch die Polizei an staatliche Gesundheitsämter gewünscht und gegen Unterschrift bestätigt wird, kann die Polizei diese Daten dem zuständigen Gesundheitsamt übermitteln.

Dies bedeutet, daß seitens der Polizei ohne Einverständnis der Betroffenen keine Übermittlungen über Selbstmordversuche mehr an Gesundheitsämter erfolgen. Von diesem Grundsatz soll nur noch dann abgewichen werden, wenn sich die betroffene Person in einem die freie Willensbestimmung ausschließenden Zustand befindet, somit ihre Ingewahrsamnahme zulässig und angemessen wäre und nach der Entlassung die Person aufgrund der Umstände des Einzelfalls durch Sorgeberechtigte oder Ehepartner/Verwandte offenkundig keinen genügenden Rückhalt finden würde.

Gegen diese Vorgehensweise bestehen aus datenschutzrechtlicher Sicht keine Bedenken.

5.4.2 Veröffentlichung personenbezogener Daten durch die Polizei in Form von Leserbriefen

Auch die Polizei darf Leserbriefe schreiben. Sie hat dabei nach Auffassung der DSK, soweit in diesen Leserbriefen personenbezogene Daten von Betroffenen enthalten sind, jedoch folgende Grundsätze zu beachten:

Als Rechtsgrundlage für die mit einem Leserbrief verbundene Datenübermittlung kommen weder die bereichsspezifischen Regelungen in den §§ 25 a ff PVG noch die allgemeinen Übermittlungsvorschriften des LDatG in Betracht, da die Übermittlung nicht der Gefahrenabwehr oder der vorbeugenden Bekämpfung von Straftaten dient und hinsichtlich der Vorschriften des LDatG davon auszugehen ist, daß die in einem Leserbrief enthaltenen personenbezogenen Daten nicht automatisiert oder in Dateien verarbeitet wurden. Als Rechtsgrundlage kann aber § 11 Landespressegesetz herangezogen werden, wonach jedermann, und damit auch Behörden, ein Gegendarstellungsanspruch zusteht. Bei der von der DSK zu beurteilenden Angelegenheit konnte sich die Polizei auf diese Vorschrift berufen, da sie zuvor, ebenfalls in Form eines Leserbriefes, von einem Betroffenen im Zusammenhang mit Rettungsmaßnahmen bei einem Verkehrsunfall massiv angegriffen wurde. Nicht beachtet wurde von der Polizei in dem der DSK vorliegenden Fall aber, daß die Gegendarstellung angemessen sein muß. Dies ergab sich daraus, daß in dem Leserbrief der Polizeibehörde Ausführungen enthalten waren, die nicht im Zusammenhang mit den Vorwürfen im zuvor veröffentlichten Leserbrief des Betroffenen standen. Die DSK hatte daher Veranlassung, darauf hinzuwirken, daß auch bei Presseveröffentlichungen durch Polizeibehörden die schutzwürdigen Belange Betroffener beachtet werden.

5.4.3 Online-Anschlüsse zwischen Polizeibehörden und dem Ausländerzentralregister

Aus einem anderen Bundesland wurde bekannt, daß zwischen Polizeibehörden und dem Ausländerzentralregister (AZR) sogenannte Online-Anschlüsse eingerichtet wurden. Da eine bereichsspezifische Rechtsgrundlage, die Datenübermittlungen aus dem AZR an Polizeidienststellen zuläßt, bisher noch nicht existiert, bestehen gegen diese Praxis Bedenken aus der Sicht des Datenschutzes. Bereichsspezifische Rechtsgrundlagen sind im Entwurf eines Ausländerzentralregistergesetzes zwar vorgesehen. Es ist jedoch nicht abzusehen, wann dieses in Kraft treten wird.

Eine Überprüfung in Rheinland-Pfalz ergab, daß hier derartige Online-Anschlüsse von Polizeibehörden zum Ausländerzentralregister nach Köln nicht bestehen. Die DSK geht davon aus, daß solche erst dann bei rheinland-pfälzischen Polizeidienststellen eingerichtet werden, wenn ausreichende bereichsspezifische Rechtsgrundlagen (Ausländerzentralregistergesetz) zur Rechtfertigung solcher Datenübermittlungen vorhanden sind.

5.4.4 Datenübermittlung an dienstvorgesetzte Stellen von öffentlich Bediensteten

Die Polizei darf dienstvorgesetzte Stellen eines Lehrers unterrichten, wenn dieser beabsichtigt, die Polizei gegenüber Schülern oder sonstigen Dritten verächtlich zu machen.

Nachdem ein gegen den Erzieher wegen einer geringfügigen Verkehrsordnungswidrigkeit erlassenes Verwarnungsgeld von der Polizei nicht aufgehoben wurde, teilte dieser dem zuständigen Polizeipräsidenten mit, daß er als „Multiplikator" in der Lage sei, andere in seiner Eigenschaft als Gymnasiallehrer darüber zu informieren, wie unangemessen er von Polizeibeamten behandelt wurde. Die Polizei unterrichtete darüber die für den Lehrer zuständige Bezirksregierung mit der Bitte, darauf hinzuwirken, daß dieser die Polizei im Rahmen seiner dienstlichen Tätigkeit nicht verächtlich macht.

Nach Auffassung der DSK ist die mit der Unterrichtung der Bezirksregierung verbundene Datenübermittlung nach § 6 Abs. 1 LDatG zulässig, da es zu den Aufgaben eines Behördenleiters gehört, zu verhindern, daß die seinem Zuständigkeitsbereich unterliegenden Bediensteten ungerechtfertigt kritisiert werden. Dabei handelt es sich um einen auch anderen Gesetzen (z. B. § 30 Abs. 4 Ziff. 5 c AO) zu entnehmenden Rechtsgedanken, wonach es keine Behörde hinzunehmen braucht, daß sie in der Öffentlichkeit in der Sache und in der Form ungerechtfertigter Kritik unterworfen wird, ohne daß sie diese Behauptungen richtigstellen kann.

5.5 Datenspeicherungen

5.5.1 Speicherung des Merkmals „Vorsicht Blutkontakt" in polizeilichen Informationssystemen

Auch in Rheinland-Pfalz werden an AIDS erkrankte Personen nicht mehr in polizeilichen Informationssystemen mit dem Merkmal „Vorsicht Blutkontakt" oder anderen Hinweisen gespeichert. Noch im 11. Tätigkeitsbericht (vgl. Tz. 8.4) hatte die DSK Veranlassung, darauf hinzuweisen, daß auch in Rheinland-Pfalz beabsichtigt sei, bei AIDS-infizierten Personen, soweit sie zur Festnahme oder Aufenthaltsermittlung ausgeschrieben waren, das Merkmal „Vorsicht Blutkontakt" zu speichern.

Gegen diese Absicht bestanden seitens der DSK erhebliche Bedenken, da bisher noch nicht überzeugend dargelegt worden ist, daß diese Speicherungen den Polizeibeamten bei ihren Einsätzen vor Ort unter dem Gesichtspunkt der Eigensicherung überhaupt nutzen können. Nach Auffassung der DSK war davon auszugehen, daß mögliche Infizierungsgefahren durch die Speicherung nicht vermindert werden, weil für die Beamten bei Einsätzen üblicherweise keine Möglichkeit besteht, vorher polizeiliche Informationssysteme abzufragen, da dies entweder aus zeitlichen (z. B. Einsatz bei einem Verkehrsunfall) oder aus anderen Gründen (die von einem Einsatz Betroffenen sind nicht bekannt) nicht möglich ist.

Nachdem das ISM zunächst der Auffassung war, die Speicherung des Merkmals „Vorsicht Blutkontakt" sei grundsätzlich zulässig, teilte es später mit, daß die Ständige Konferenz der Innenminister und -senatoren der Länder beschlossen habe, die Speicherung von Hinweisen auf eine HIV-Infektion in das Ermessen des Bundes oder jeweiligen Landes zu stellen. Für die Polizei des Landes Rheinland-Pfalz ist daraufhin angeordnet worden, die Speicherung von Informationen, die auf eine HIV-Infektion schließen lassen, mit sofortiger Wirkung einzustellen. Bereits gespeicherte Informationen wurden gelöscht.

Diese Entscheidung gilt auch für Vermerke über eine HIV-Infektion in Akten.

Die Bereinigung der Akten wurde nach Auskunft des ISM bis Ende 1988 abgeschlossen.

Die DSK begrüßt die Entscheidung. Denn eine zuvor durchgeführte Überprüfung von Kriminalakten hatte ergeben, daß der Hinweis auf eine AIDS-Infektion meist auf ausgesprochen unzuverlässigen Informationen beruhte.

5.5.2 Speicherung des personengebundenen Hinweises (PHW) „Prostitution" in POLIS

Die DSK überprüfte im Berichtszeitraum die Speicherung des PHW „Prostitution" in POLIS. Dabei ergab sich kein Anlaß zu Beanstandungen. Allen überprüften Akten waren ausreichende Hinweise zu entnehmen, daß die Personen tatsächlich der Prostitution nachgehen. Die Akten waren wegen im Rahmen der Prostitution begangener Delikte angelegt worden.

Üblicherweise beruhte die Speicherung des PHW auf eigenen Angaben der Betroffenen, vereinzelt auch auf Feststellungen der Polizeibeamten. Vage, beispielsweise lediglich aus dem Milieu stammende Hinweise führten nicht zur Speicherung des PHW.

Im Rahmen dieser örtlichen Feststellungen wurde die Frage angesprochen, ob es zulässig ist, daß über betroffene Prostituierte personenbezogene Daten gespeichert, Akten angelegt und ED-Behandlungen durchgeführt werden, wenn diese sich freiwillig bei der Polizei melden, ohne daß der Polizei sonstige, eine Speicherung rechtfertigende Informationen bekannt sind.

Dies war bisher eine bei vielen Polizeidienststellen übliche Praxis. Dabei ist zu berücksichtigen, daß die personenbezogenen Daten jeder Prostituierten, die sich einer solchen ED-Behandlung unterziehen, in POLIS eingestellt werden mit der Folge, daß die Daten landesweit abrufbar sind.

Bei der DSK bestanden Zweifel, ob bei den Betroffenen tatsächlich von einer Freiwilligkeit ausgegangen werden kann und ob die §§ 11, 25 a PVG nicht als abschließende Regelung anzusehen sind, so daß dann, wenn die dort normierten Voraussetzungen nicht vorliegen, auch aufgrund einer Einwilligung des Betroffenen keine Maßnahmen (ED-Behandlung, Speicherung) zulässig sind, obwohl § 5 LDatG Speicherungen auch aufgrund einer Einwilligung zuläßt.

Nachdem die mit der Durchführung dieser ED-Behandlung verbundenen Fragen im Rahmen örtlicher Feststellungen bei einer Polizeidienststelle besprochen worden waren, teilte das ISM anschließend mit, daß eine erkennungsdienstliche Behandlung von Prostituierten auf freiwilliger Basis in Rheinland-Pfalz nicht mehr erfolgen wird, da diese Maßnahme von der gesetzlichen Aufgabenzuweisung für die Polizei nicht erfaßt sei und die Polizei im übrigen nicht nachprüfen kann, ob sich die Betroffene tatsächlich freiwillig erkennungsdienstlich behandeln läßt oder ob die Prostituierte nur dem Druck eines Bordellbetreibers ausgesetzt ist, der die Frauen als Geste des Wohlverhaltens gegenüber der Polizei zu einer erkennungsdienstlichen Behandlung schickt.

5.6 Überprüfung polizeilicher Staatsschutzabteilungen

Sog. Blockierer von Raketenstandorten (z. B. Hasselbach) werden von der Polizei in der „Arbeitsdatei PIOS Innere Sicherheit" (APIS) nicht mehr gespeichert. Das ist eines der Ergebnisse, die im Rahmen der bereits im 11. Tätigkeitsbericht (vgl. Tz. 4.2) angesprochenen Überprüfung polizeilicher Staatsschutzabteilungen erzielt werden konnten.

Der von der DSK vertretenen Auffassung, wonach die in APIS vorgenommene Speicherung personenbezogener Daten sog. Blockierer unzulässig ist, hatte das ISM zunächst widersprochen. Es vertrat die Auffassung, daß das Verhalten der Blockierer als eine Straftat anzusehen ist, die sich gegen die freiheitlich demokratische Grundordnung richtet. Bei dieser Bewertung sei davon auszugehen, daß die Blockadeteilnehmer mit dem Versperren der Zu- und Abfahrt nicht nur das Ziel verfolgten, durch kollektives Verhalten auf die nach ihrer Auffassung nicht gerechtfertigte Nachrüstung hinzuweisen und die Öffentlichkeit für ihren Standpunkt zu mobilisieren, sondern daß sie letztlich Druck auf die Bundesregierung als Verfassungsorgan ausüben wollten.

Zu einem späteren Zeitpunkt schloß sich das ISM jedoch der von der DSK vertretenen Auffassung an und beauftragte das Landeskriminalamt, alle Speicherungen von Personen in APIS, denen Straftaten im Zusammenhang mit der Blockadeaktion vorgeworfen wurden, unter Zugrundelegung der von der DSK entwickelten Grundsätze zu überprüfen.

Nach Abschluß dieser internen polizeilichen Überprüfung wurde der DSK mitgeteilt, daß alle Speicherungen im Zusammenhang mit Blockadeaktionen in APIS gelöscht worden seien und daß zu diesen Ereignissen in APIS nunmehr kein Datenbestand mehr vorhanden sei.

5.7 Friedensinitiative vom Staatsschutz observiert?

Der zunächst entstandene Eindruck, eine in einer rheinland-pfälzischen Stadt aktive Friedensinitiative werde vom Staatsschutz observiert, hat sich nicht bestätigt. Der DSK wurde ein Fernschreiben der Polizei mit der Bitte um Überprüfung vorgelegt, in dem u. a. die Information enthalten war, daß ein Betroffener, der im Zusammenhang mit einer Straftat aufgefallen war, im „Arbeitskreis Frieden" aktiv sei. Im übrigen, so das Fernschreiben, sei er Bezieher der Zeitschrift „radikal".

Gegen die Übermittlung der Information über den Bezug dieser Zeitschrift waren keine Bedenken zu erheben, da es sich dabei um eine Druckschrift handelt, die häufig wegen des Verdachts der damit verbundenen Unterstützung einer terroristischen Ver-

einigung beschlagnahmt wurde. Die Übermittlung dieses Hinweises an andere Polizeidienststellen war zur vorbeugenden Bekämpfung von Straftaten nach § 25 a PVG zulässig, da er dazu dienen kann, zukünftige Straftaten nach §§ 129, 129 a StGB bzw. § 20 Ziff. 4 Landespressegesetz (Verbreitung beschlagnahmter Druckwerke) schneller aufzuklären.

Bedenken wurden von der DSK gegen die Übermittlung des Hinweises „Mitglied in der Friedensinitiative Worms" im Fernschreiben der Polizeidirektion geäußert, da dafür nach Auffassung der DSK weder ein Polizeibezug noch eine Erforderlichkeit für das anhängende Strafverfahren festzustellen war. Bereits vor Äußerung dieser Bedenken war die DSK vom ISM darüber informiert worden, daß von der Polizei eine Löschung dieses Datums in den an verschiedene Adressaten gerichteten Fernschreiben nachträglich veranlaßt worden war.

Festgestellt werden konnte von der DSK jedenfalls, daß betreffend der Friedensinitiative keine Observationsmaßnahmen stattgefunden hatten. Dem das Fernschreiben veranlassenden Polizeibeamten war die Mitgliedschaft des Betroffenen in der Friedensinitiative zufällig bekannt geworden (sog. privates Wissen).

5.8 Tieffluggegner im Visier des polizeilichen Staatsschutzes?

Auch dieser Frage hatte die DSK im Berichtszeitraum nachzugehen. Anlaß war ein der DSK vorliegendes Fernschreiben einer Polizeidienststelle, dem u. a. folgendes entnommen werden konnte:

„Die überparteiliche Interessengemeinschaft der Bürgermeisterinnen und Bürgermeister gegen den Fluglärm beschloß Mitte Juni 1988 in Eisenberg, am 28. Juni 1988 mit einem Mahn- und Protesttag gegen den Fluglärm zu protestieren. Diesem Protest haben sich mit Unterstützung der SPD-Landtagsfraktion 45 Städte und Gemeinden in der Pfalz und in Rheinhessen angeschlossen. Der Verbandsbürgermeister aus . . . rief Anfang Juni 1988 zu Unterschriftensammlungen und Aktionen mit Luftballons gegen den Tiefflugverkehr in der Vorderpfalz auf."

Im Rahmen einer von der DSK durchgeführten Überprüfung konnte nicht festgestellt werden, daß personenbezogene Daten von rheinland-pfälzischen Bürgermeistern, Mitgliedern der SPD-Landtagsfraktion oder Angehöriger anderer Landtagsfraktionen in automatisierten polizeilichen Dateien gespeichert werden. Die Erwähnung der SPD-Landtagsfraktionen in dem in einem Schreibautomaten gespeicherten Einsatzbefehl hatte keine datenschutzrechtliche Relevanz, da es sich dabei nicht um ein personenbezogenes Datum im Sinne des § 3 Abs. 1 LDatG handelt. Bedenken bestanden jedoch gegen die Erwähnung des Verbandsbürgermeisters aus . . . in diesem Einsatzbefehl, da es sich dabei um ein personenbezogenes Datum handelt, das erhoben und übermittelt (u. a. auch an den Verfassungsschutz) wurde. Nach Auffassung der DSK war es fraglich, ob die Erhebung dieses Datums zur Abwehr einer konkreten Gefahr (§ 25 a Abs. 1 Ziff. 1 PVG) und die Übermittlung an den Verfassungsschutz zur rechtmäßigen Erfüllung der in dessen Zuständigkeit liegenden Aufgaben erforderlich war. Diese Bedenken wurden dem ISM seitens der DSK mitgeteilt.

Schließlich konnte festgestellt werden, daß aktenmäßig bei der zuständigen Polizeidienststelle eine umfassende Dokumentation über die Aktivitäten von Initiativen gegen die Heeresübung „Landesverteidigung 88" bzw. gegen den Tiefflugläm angelegt wurde, soweit es sich dabei um öffentlich zugängliche Informationen (insbesondere Presseartikel) handelte. In dieser Sammlung waren u. a. auch zwei Zeitungsartikel enthalten, die sich mit dem Beschluß der SPD-Landtagsfraktion befaßten, der zur Unterstützung der Aktion „Bürgermeister gegen den Tiefflugläm" gefaßt worden war. Obwohl es sich bei diesen Unterlagen um öffentlich zugängliche Materialien handelte, dürfen auch diese nur unter der Voraussetzung des § 25 a Abs. 1 PVG „erhoben" werden, soweit in ihnen (auch) personenbezogene Daten enthalten sind. Die DSK hatte Bedenken, ob diese lückenlose Sammlung zur Gefahrenabwehr erforderlich war. Auch diese Bedenken wurden dem ISM mitgeteilt.

Bereits vorher war der DSK von den zuständigen Mitarbeitern der Polizei zugesichert worden, daß diese Sammlung von Unterlagen umgehend vernichtet wird.

5.9 Musterdienstanweisung über den Datenschutz und die Datensicherheit bei der Polizei

Auch für den Polizeibereich liegt nunmehr die von § 9 LDatG geforderte Dienstanweisung über technische und organisatorische Sicherungsmaßnahmen beim EDV-Einsatz vor.

Im Berichtszeitraum wurde der DSK der erste Entwurf einer solchen Dienstanweisung vorgelegt. Zwischen den Vertretern des ISM und der DSK fanden Gespräche statt, in denen dieser Entwurf erörtert und den Notwendigkeiten eines effektiven Datenschutzes angepaßt wurde. Die Dienstanweisung trat am 20. März 1989 in Kraft. In ihr sind nunmehr die von § 9 Abs. 1 Satz 2 in Verbindung mit § 1 der „Landesverordnung über technische und organisatorische Datenschutzanforderungen nach § 9 des LDatG" normierten Regelungen zur Datensicherung enthalten.

Soweit beim Einsatz der EDV bei einzelnen Polizeidienststellen ergänzende Sicherungsmaßnahmen erforderlich werden, sind diese zusätzlich noch in die Dienstanweisung aufzunehmen.

5.10 Übermittlung unzutreffender Informationen durch die Polizei

Die Polizei darf nur solche Informationen an andere Dienststellen übermitteln, die auch zutreffend sind. Die DSK hat Veranlassung, darauf erneut hinzuweisen. Anlaß dafür ist die Eingabe eines Petenten, der sich bei der DSK darüber beschwerte, daß in einem polizeilichen Fernschreiben der auf seine Person bezogene Hinweis enthalten war, er sei „einschlägig wegen sicherheitsgefährdendem Abbildens" von militärischen Anlagen bekannt.

Die Überprüfung der DSK ergab, daß zwar zahlreiche Ermittlungsverfahren gegen den Petenten wegen des Verdachts des sicherheitgefährdendem Abbildens von militärischen Anlagen eingeleitet wurden, die jedoch alle mangels Vorliegens eines Tatverdachts eingestellt wurden (§ 170 Abs. II StPO). In keinem der Fälle waren militärische Sicherheitsinteressen gefährdet.

Daraus ergab sich, daß die in dem Fernschreiben enthaltene Behauptung unzutreffend war.

Diese Eingabe zeigt erneut, wie wichtig es ist, daß seitens der Staatsanwaltschaft eine Rückmeldung über den Ausgang der Verfahren an die für die Speicherung verantwortlichen Stellen (Polizei) erfolgt. Nur so können diese Stellen prüfen, ob die Speicherung weiter aufrecht zu erhalten oder ob eine Löschung vorzunehmen ist. Dieser Fall zeigt aber auch, daß seitens der Polizei Anstrengungen zu unternehmen sind, in Erfahrung zu bringen, wie die Verfahren von den Justizbehörden beendet wurden. Aufgrund der von der DSK mittlerweile gewonnenen Erfahrungen kann nicht davon ausgegangen werden, daß die Rückmeldung durch die Justizbehörden reibungslos verläuft (vgl. hierzu auch Tz. 7.3.5).

Schließlich hat die Polizei darauf zu achten, daß von ihr vorgenommene Speicherungen immer dann zu löschen sind, wenn die Akte mangels Vorliegens eines weiteren Verdachts nicht an die Staatsanwaltschaft abgegeben wird.

6 Verfassungsschutz

6.1 Vorbemerkung

Die Berichterstattung aus dem Bereich Verfassungsschutz kann die Tätigkeit der DSK in diesem Gebiet nicht vollständig wiedergeben, da ein umfangreicher Teil der datenschutzrechtlich relevanten Vorgänge dieser Behörde naturgemäß als Verschlußsache eingestuft ist und sich somit der Darstellung in der Öffentlichkeit entzieht.

Im Schwerpunkt lag die Überprüfungstätigkeit der DSK im Sicherheitsbereich ohnehin bei der Polizei. Dort haben die Datenschutzbeauftragten und die DSK im Berichtszeitraum in Abstimmung miteinander eine Überprüfung der Staatsschutzabteilungen durchgeführt (vgl. Tz. 5.6 u. 11. Tätigkeitsbericht Tz. 4.2) und beendet.

Eine solche abgestimmte Überprüfung für den Verfassungsschutz ist im Jahr 1990 vorgesehen.

Gravierende Verstöße des Verfassungsschutzes gegen datenschutzrechtliche Vorschriften waren nicht festzustellen. Dies schließt nicht aus, daß unterschiedliche Auffassungen zu einzelnen Fragen bestanden. Die wesentlichen Diskussionspunkte werden im folgenden dargestellt.

Nicht abzusehen ist, ob in der gegenwärtigen Legislaturperiode der in den Bundestag eingebrachte Entwurf eines Bundesverfassungsschutzgesetzes noch verabschiedet wird. Sowohl zu diesem wie auch zum Entwurf eines MAD-Gesetzes und eines BND-Gesetzes hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission eine Entschließung vom 30. Mai 1989 verabschiedet, die in der Anlage (vgl. Anlage 3) abgedruckt ist.

6.2 Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes (Sicherheitsrichtlinien)

Die DSK erhielt rechtzeitig Gelegenheit, zum Entwurf der Richtlinien Stellung zu nehmen.

Gegenstand der Sicherheitsrichtlinien ist der sog. personelle Geheimschutz, insbesondere die Sicherheitsüberprüfung von Personen in sicherheitsempfindlicher Tätigkeit. Die Richtlinien gelten für die Landesbehörden, die Kommunalbehörden sowie die der Aufsicht des Landes unterstehenden Körperschaften des öffentlichen Rechts und rechtsfähigen Anstalten und Stiftungen des öffentlichen Rechts. Über Personen, die sich einer Sicherheitsüberprüfung zu unterziehen haben, weil sie eine sicherheitsempfindliche Tätigkeit ausüben sollen, werden in erheblichem Umfang personenbezogene Daten durch staatliche Stellen erhoben. In mehreren Gesprächen mit den Vertretern des ISM konnten folgende Verbesserungen hinsichtlich des Datenschutzes erreicht werden:

a) Auf die Möglichkeit, Betroffene nach „anderen Personen des näheren Lebensumfeldes" zu befragen, wurde wegen der Unbestimmtheit dieses Begriffs verzichtet.

b) Die Auffassung der DSK, wonach der sog. Übergangsbonus (vgl. 11. Tätigkeitsbericht, Tz. 2) nach dem Volkszählungsurteil des BVerfG nur noch ganz befristet gelten kann, fand in geeigneter Form Eingang in die Richtlinien.

c) Ebenfalls auf Anregung der DSK wird in den Richtlinien darauf hingewiesen, daß zur Feststellung und Aufkärung von Umständen, die auf ein Sicherheitsrisiko hindeuten können, keine nachrichtendienstlichen Mittel eingesetzt werden dürfen.

d) Anfragen an private Stellen im Rahmen der Sicherheitsüberprüfungen werden grundsätzlich nicht erfolgen.

e) Eine Verlängerung der Aufbewahrungsfrist von Unterlagen bei „sicherheitserheblichen Erkenntnissen" ist entfallen. Ergänzend wurde geregelt, daß eine Vernichtung der Sicherheitsakten spätestens nach zwei Jahren zu erfolgen hat, wenn eine Sicherheitsüberprüfung nicht zu Ende geführt wurde, etwa weil der Betroffene seine Bewerbung zurückgezogen hat.

f) Eine Unterrichtung des behördlichen Geheimschutzbeauftragten durch die personalverwaltende Stelle über Straftaten oder Dienstordnungsfälle des sicherheitsüberprüften Bediensteten darf nur noch erfolgen, wenn ein sicherheitsrelevanter Bezug festzustellen ist.

g) Im Interesse der Transparenz wurde von der DSK gefordert und vom ISM akzeptiert, daß die automatisierte Datei, in die personenbezogene Daten im Zusammenhang mit der Durchführung der Sicherheitsüberprüfungen gespeichert werden, in den Richtlinien ausdrücklich bezeichnet wird (NADIS).

h) Erreicht werden konnte ebenfalls, daß die behördlichen Geheimschutzbeauftragten, die die Sicherheitsüberprüfungen federführend durchführen, bis zum Erlaß bereichs spezifischer Regelungen in einem Geheimschutzgesetz keine personenbezogenen Daten aus den Sicherheitsüberprüfungen in automatisierten Systemen speichern dürfen, weil zur Zeit hierfür die erforderliche hinreichend bestimmte Rechtsgrundlage fehlt.

i) Bei der Überprüfung möglicher Mitgliedschaften in verfassungsfeindlichen Organisationen wird der Betroffene darauf hingewiesen, daß ihm zur Information über die Frage, welche Organisation als verfassungsfeindlich anzusehen ist, der jeweils letzte Verfassungsschutzbericht zur Verfügung steht. Der Betroffene wird aufgrund einer Anregung der DSK ebenfalls schriftlich darüber aufgeklärt, daß er nicht verpflichtet ist, Angaben zu machen, die zu einer strafrechtlichen Verfolgung führen können.

j) Weiterhin wird in den Richtlinien festgehalten, daß die DSK nicht nur die Dateien kontrollieren kann, sondern daß sie auch ein Recht zur Einsicht in die zu den Speicherungen geführten Sicherheitsakten hat. Ebenfalls wird ergänzend in den Richtlinien das Kontrollrecht der DSK zur Überprüfung der vorgenommenen Datenübermittlungen und der rechtzeitigen Löschung von Daten ausdrücklich genannt.

k) Schließlich sollen die Betroffenen darauf hingewiesen werden, daß sie sich zur Überprüfung der datenschutzrelevanten Vorgänge im Rahmen der Sicherheitsüberprüfung auch an die DSK wenden können.

6.3 Rechtsverordnung über die Überprüfung von Dateien des Verfassungsschutzes auf ihre Erforderlichkeit

Nach § 8 Abs. 1 des Landesverfassungsschutzgesetzes vom 26. März 1986 sind Dateien des Verfassungsschutzes in regelmäßigen Abständen auf ihre Erforderlichkeit zu überprüfen. Die regelmäßigen Abstände der Überprüfung sind durch Rechtsverordnung der Landesregierung festzulegen. Im April 1988 fragte die DSK beim ISM nach, wann mit dem Erlaß der Rechtsverordnung gerechnet werden könne.

Aufgrund dieser Anfrage der DSK leitete ihr das ISM den Entwurf einer Landesverordnung über die regelmäßigen Überprüfungsabstände der Dateien des Verfassungsschutzes mit der Bitte um Stellungnahme zu. Nach diesem Entwurf sind die Dateien des Verfassungsschutzes in regelmäßigen Abständen von fünf Jahren auf ihre Erforderlichkeit zu überprüfen. Die erstmalige Überprüfung erfolgt zum 20. Januar 1990. Die weiteren Überprüfungen sind bis zum 20. Januar des jeweils folgenden fünften Jahres abzuschließen. Das Ergebnis der Überprüfung ist schriftlich niederzulegen, zu begründen und von einem Mitarbeiter des höheren Dienstes verantwortlich zu unterzeichnen.

Materielle Bedenken hat die DSK nicht erhoben. Die Landesverordnung ist am 29. Mai 1989 in Kraft getreten (GVBl. S. 163).

6.4 Überprüfung der besonderen technischen Mittel zur verdeckten Informationserhebung bei Polizei und Verfassungsschutz

Verfassungsschutz und Polizei dürfen besondere technische Mittel zur verdeckten Informationserhebung nur unter besonderen Voraussetzungen einsetzen (§ 5 LVerfSchG/§ 25 b PVG). Das ISM wurde von der DSK gebeten, ihr zu Überprüfungszwecken

mitzuteilen, um welche technischen Mittel es sich dabei im einzelnen handelt. Für den Bereich der Polizei führte das ISM unter beispielhafter Aufzählung einiger der eingesetzten technischen Mittel aus, daß eine abschließende Aufzählung dieser Einsatzmittel wegen der ständig fortschreitenden technischen Entwicklung nicht möglich sei. Für den Bereich des Verfassungsschutzes erfolgte nur eine beispielhafte Aufzählung einiger eingesetzter Geräte, ohne nähere Einzelangaben. Eine Konkretisierung der Angaben wurde nicht vorgenommen.

Die DSK ist nach wie vor der Auffassung, daß ihr gesetzlicher Informationsanspruch auch die Erteilung der zusätzlich erbetenen Auskünfte sowie die Präsentation der eingesetzten Mittel umfaßt (§ 20 LDatG).

Nach § 17 Abs. 1 LDatG hat die DSK die Aufgabe, die Einhaltung auch „anderer Vorschriften über den Datenschutz" zu überwachen. Die Voraussetzungen, unter denen die Polizei und der Verfassungsschutz technische Mittel zur verdeckten Informationserhebung einsetzen dürfen, sind in den §§ 25 a Abs. 2, 25 b Abs. 1 PVG bzw. § 5 LVerfSchG geregelt. Diese Vorschriften treffen Aussagen darüber, wann (derartige) Eingriffe in das Recht auf informationelle Selbstbestimmung Betroffener vorgenommen werden dürfen. Es handelt sich somit um „andere Vorschriften über den Datenschutz".

Nachdem diese Gesichtspunkte dem Innenminister vorgetragen wurden, erklärte er sein Einverständnis, die von der Polizei eingesetzen technischen Mittel der DSK zu präsentieren; dies könne jedoch für den Bereich des Verfassungsschutzes nicht erfolgen. Er begründete dies u. a. wie folgt: „Ich mußte bei dieser Entscheidung berücksichtigen, daß die technischen Mittel des Verfassungsschutzes in einem weitaus größeren Umfang mehr geheimhaltungsbedürftig sind als die von der Polizei eingesetzten Mittel. Viele technische Mittel des Verfassungsschutzes sind nicht handelsübliche Gegenstände und zu einem großen Teil, auf die speziellen konspirativen Arbeitsumstände abgestellt, durch eigene Kräfte hergestellt worden. Schon die konkrete Bezeichnung jedes einzelnen zum Einsatz kommenden technischen Mittels und erst recht eine Vorführung aller Geräte eröffnet einen tiefen Einblick in die Arbeitsmethoden und den Stand der nachrichtendienstlichen Technik." Ohne ihren Rechtsstandpunkt aufzugeben, schloß sich die DSK im Interesse der stets von Sachlichkeit geprägten guten Zusammenarbeit mit dem ISM dem Vorschlag des Ministers an, entsprechende Überprüfungen im Bereich des Verfassungsschutzes nur anlaßbezogen durchzuführen, soweit dadurch die Kontrollbefugnisse der DSK nicht beeinträchtigt werden.

Die Überprüfung der von der Polizei eingesetzten technischen Mittel ist inzwischen erfolgt. Die DSK hat damit eine Basis für künftige konkrete Einzelfallprüfungen in diesem Bereich gewonnen.

6.5 Einsichtsrecht in Akten des Verfassungsschutzes

Bei der Bearbeitung einer Eingabe kam es zu einer unterschiedlichen Auslegung der Bestimmung des § 20 LDatG über den Umfang des Rechts auf Einsichtnahme in über Betroffene beim Verfassungsschutz angelegte Akten, ohne daß eine Speicherung in automatisierten Systemen vorgelegen hat.

Vom ISM wurde die Auffassung vertreten, daß derzeit ein solches Einsichtsrecht der DSK nicht bestehe. Dies ergebe sich aus § 2 Abs. 2 LDatG, wonach die Bestimmungen des Landesdatenschutzgesetzes nur dann gelten, wenn personenbezogene Daten in Dateien gespeichert, verändert oder übermittelt würden. Auch in § 3 Abs. 3 Nr. 3 LDatG werde der Dateibegriff genau definiert. Dort sei geregelt, daß zum Dateibegriff weder Akten noch Aktensammlungen gehörten, es sei denn, daß sie durch automatisierte Verfahren umgeordnet oder ausgewertet werden könnten. Eine solche Umordnungsmöglichkeit gebe es jedoch für die Akten des Verfassungsschutzes in Rheinland-Pfalz nicht. Daher gehe man davon aus, daß vom LDatG nur personenbezogene Daten in Dateien geschützt werden sollen.

Die DSK vertritt im Gegensatz dazu – wie schon immer – die Auffassung, daß ihr bei einer verfassungskonformen Auslegung der genannten gesetzlichen Bestimmungen unter Berücksichtigung der Grundsätze, die das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 aufgestellt hat, ein Einsichtsrecht in Akten und Unterlagen, unabhängig vom Dateibezug, zusteht. Dies gelte jedenfalls immer dann, wenn sich ein Bürger an die DSK wende. Selbstverständlich bleibt das Recht des Ministers, im Einzelfall diese Akteneinsicht wegen einer Gefährdung der Sicherheit des Bundes oder des Landes gem. § 20 LDatG zu untersagen, unberührt. In einem Gespräch mit der DSK äußerte der Minister des Innern und für Sport in diesem Zusammenhang, daß er zwar grundsätzlich an der bisher vom Verfassungsschutz vertretenen Auffassung festhalte, schlug aber im Interesse der guten Zusammenarbeit vor,

- der Auskunftssuchende müsse hinreichend Anhaltspunkte darlegen, weshalb er sich in seinen Rechten verletzt fühlt,
- dem Innenministerium seien diese Gründe mitzuteilen.

In diesen Einzelfällen behalte er sich die Entscheidung vor, ob trotz Fehlens einer Speicherung in automatisierten Systemen Einsicht in Akten des Verfassungsschutzes genommen werden kann. Die DSK akzeptierte unter Aufrechterhaltung ihres bisher vertretenen Rechtsstandpunktes im Interesse der weiteren Zusammenarbeit diesen Vorschlag.

6.6 Erteilung von Auskünften durch den Verfassungsschutz an (möglicherweise) Betroffene

In Kenntnis einer Entscheidung des OVG Bremen vom 24. Februar 1987 (Az: 1 BA 50/86), in der ausgeführt wurde, daß der Verfassungsschutz trotz der vom Gesetz eingeräumten Möglichkeit der Auskunftsverweigerung nicht generell Auskünfte verweigern darf, befaßte sich die DSK mit der Auskunftspraxis des rheinland-pfälzischen Verfassungsschutzes. Das um Stellungnahme gebetene Ministerium verblieb bei der Auffassung, daß aufgrund des § 10 LVerfSchG für den Verfassungsschutz keine Verpflichtung bestehe, an anfragende Personen Auskunft zu erteilen. Eine Auskunftserteilung bleibe zwar möglich und sei auch schon erfolgt, sie könne aber nur dann in Betracht gezogen werden, wenn ein Ausforschungsversuch sicher ausgeschlossen werden könne.

Die DSK vertritt demgegenüber folgende Standpunkte:

- Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum mehr, jede Speicherung personenbezogener Daten durch staatliche Stellen stellt einen Grundrechtseingriff dar, der auch am Verhältnismäßigkeitsprinzip zu messen ist.

- Ob die Voraussetzungen für die Rechtmäßigkeit eines Informationseingriffes vorliegen, muß wegen des durch Art. 19 Abs. 4 Grundgesetz dem Einzelnen gewährleisteten möglichst lückenlosen Rechtsschutzes der Kontrolle durch ein Gericht unterliegen.

  Voraussetzung für die Inanspruchnahme des gerichtlichen Rechtsschutzes ist jedoch, daß der Betroffene weiß, ob und was über ihn bei staatlichen Stellen gespeichert ist. Der Auskunftsanspruch ist daher eine wesentliche verfahrensrechtliche Regelung zum Schutz des Rechts auf informationelle Selbstbestimmung. Beschränkungen des Auskunftsrechts bedürfen der für Beschränkungen des Rechts auf informationelle Selbstbestimmung aufgestellten Voraussetzungen.

- Vorschriften, die sich wie § 10 LVerfSchG auf die Erteilung von Auskünften beziehen, sind daher verfassungskonform auszulegen. Dabei sind das Recht auf informationelle Selbstbestimmung und die verfassungsrechtliche Rechtsschutzgarantie zugrunde zu legen. Der hohe Rang dieser Verfassungsnormen verlangt zwingend, daß das informationelle Selbstbestimmungsrecht des Bürgers dem Geheimhaltungsinteresse des Verfassungsschutzes nicht generell untergeordnet wird. Ohne Auskunft können Grundrechtsverstöße nicht festgestellt und nicht gerichtlich geltend gemacht werden. Wegen dieser verfassungsrechtlichen Bedeutung untersteht auch im Sicherheitsbereich die behördliche Entscheidung über ein Auskunftsbegehren des Betroffenen dem grundrechtlich legitimierten Verhältnismäßigkeitsprinzip. Durch eine Güterabwägung ist in jedem konkreten Fall zu ermitteln, ob das behördliche Geheimhaltungsinteresse nach der Gestaltung des Einzelfalls zwingend den Vorrang vor den Grundrechts- und Rechtsschutzinteressen des Betroffenen verdient. Danach ist eine Auskunftsverweigerung nur dann rechtmäßig, wenn sie dem gesetzlichen Zweck des Verfassungsschutzes dient, zur Erreichung dieses Zwecks geeignet und erforderlich und für den Betroffenen zumutbar ist.

- Für eine an den unterschiedlichen Zwecken des Verfassungsschutzes und am Verhältnismäßigkeitsprinzip orientierte rechtliche Bewertung des behördlichen Geheimhaltungsinteresses liegt eine Unterscheidung nach Aufgabengebieten nahe.

  Informationen über Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen verfolgt werden oder über geheimdienstliche Tätigkeiten werden in der Regel strikter Geheimhaltung bedürfen. Bei Informationen über sonstige Bestrebungen (Extremismusbeobachtung) ist eine differenzierte Sichtweise erforderlich:

  Bei einem auf einen bestimmten Tatbestand bezogenen Auskunftsbegehren – namentlich bei länger zurückliegenden und abgeschlossenen Tatbeständen, zumal wenn die gespeicherten Informationen auf allgemein zugänglichen oder amtlichen Quellen beruhen oder wenn der Anfragende weiß oder vermutet, daß Informationen über ihn gespeichert sind –, ist eine Ausforschungsgefahr regelmäßig nicht zu befürchten. Soll die Auskunft gleichwohl verweigert werden, müssen dafür triftige Gründe bestehen und einleuchtend dargelegt werden. Werden im Antragsverfahren besondere Umstände deutlich, die ein gesteigertes Auskunftsinteresse des Antragstellers begründen – solche Umstände können z. B. die erschwerte Arbeitsplatzsuche, drohender Arbeitsplatzverlust, gesundheitliche Beeinträchtigung, Herabsetzung seines Bildes in der Öffentlichkeit sein –, so muß die Verfassungsschutzbehörde besonders sorgfältig abwägen, ob ein bestehendes Geheimhaltungsinteresse die mit einer Auskunftsverweigerung verbundenen persönlichen Belastungen des betroffenen Bürgers rechtfertigen kann. Auch bei dieser Fallgruppe der konkreten und besonderen Betroffenheit des Antragstellers muß der Verfassungsschutz eine etwaige Auskunftsverweigerung so plausibel begründen, daß eine wirksame gerichtliche Überprüfung seiner Entscheidungen möglich bleibt.

Der rheinland-pfälzische Verfassungsschutz konnte sich bisher der Auffassung der DSK nicht anschließen.

6.7 Sog. Regelanfragen von Kreditinstituten beim Verfassungsschutz

Bei Prüfung einer Eingabe stellte die DSK fest, daß auch von Sparkassen bei der Einstellung von Mitarbeitern gem. § 7 Abs. 3 LVerfSchG Regelanfragen an den rheinland-pfälzischen Verfassungsschutz gestellt werden. Die DSK hatte die Frage zu prüfen, ob solche Anfragen von öffentlich-rechtlichen Kreditinstituten an den Verfassungsschutz zulässig sind.

Nach § 7 Abs. 3 LVerfSchG erteilt der Verfassungsschutz auf Anfrage von Behörden, denen die Einstellung von Bewerbern in den öffentlichen Dienst obliegt, nach pflichtgemäßen Ermessen Auskunft aus vorhandenen Unterlagen.

Die Tätigkeit einer Sparkasse ist bei öffentlich-rechtlicher Trägerschaft dem öffentlichen Dienst zuzurechnen. Die Bediensteten gehören als Beamte oder BAT-Angestellte dem öffentlichen Dienst an. Die politische Treuepflicht gilt nicht nur für Beamte, sondern auch für Angestellte im öffentlichen Dienst (§ 5 BAT). Da die DSK bei Regelanfragen von öffentlich-rechtlichen Kreditinstituten auch keinen Verstoß gegen den Gleichheitsgrundsatz sah, (Regelanfragen durch private Kreditinstitute sind zwar nicht möglich, dadurch entsteht aber kein Wettbewerbsvorteil für diese Institute), bestanden im Ergebnis keine Bedenken gegen die Zulässigkeit solcher Anfragen von Sparkassen an den Verfassungsschutz.

Bei der Überprüfung dieser Frage konnte jedoch festgestellt werden, daß die in der Eingabe genannte Sparkasse die Anfrage bei einem Bewerber um eine Ausbildungsstelle vorgenommen hatte.

Dies verstieß gegen Ziffer 2.1 der VV des ISM vom 12. Dezember 1985 (MinBl. 1986, S. 178), da dieser Verwaltungsvorschrift zu entnehmen ist, daß eine Anfrage bei Personen, die im öffentlichen Dienst ausgebildet werden, erst nach Abschluß der Ausbildung erfolgen darf, soweit beabsichtigt ist, diese weiter zu beschäftigen. Die DSK hat daher Veranlassung, ausdrücklich darauf hinzuweisen, daß bei Bewerbern um eine Ausbildungsstelle im öffentlichen Dienst Regelanfragen an den Verfassungsschutz unzulässig sind.

7 Justiz

7.1 Vorbemerkung

Die Justiz war lange ein Bereich, in dem die automatisierte Datenverarbeitung eine eher geringe Rolle gespielt hat. Ihr Einsatz hatte sich auf wenige Gebiete (z. B. das Grundbuchwesen) beschränkt, eine flächendeckende Einführung ist selbst hier nur langsam vorangeschritten.

Dies hat sich im Berichtszeitraum grundlegend gewandelt. Immer mehr Tätigkeitsbereiche innerhalb der Justiz nutzen die Automationsunterstützung. Zentrale Systeme (z. B. im Mahnverfahren und bei der staatsanwaltschaftlichen Tätigkeit), die in relativ kurzer Zeit flächendeckend eingesetzt werden sollen, gewinnen große Bedeutung. Hinzu kommt das Vordringen dezentraler DV-Systeme, die im Kernbereich staatsanwaltschaftlicher und richterlicher Tätigkeit vermehrt Einsatz finden. Die damit einhergehenden datenschutzrechtlichen Fragen sind noch nicht gelöst: Die DSK hat sich zwar punktuell mit einer Reihe entsprechender Verfahren befaßt, die damit im Zusammenhang stehenden grundsätzlichen Fragen sind jedoch vom Gesetzgeber zu entscheiden, der bislang noch nicht die notwendigen Regelungen getroffen hat. Eine Reihe von Gesetzesentwürfen liegt zwar vor: z. B. für die Datenverarbeitung im Zusammenhang mit dem Strafprozeß, für Datenübermittlungen zwischen gerichtlichen Stellen (Justizmitteilungsgesetzentwurf), für die Führung des Schuldnerverzeichnisses, für die Datenverarbeitung im Strafvollzug. Die Gesetzgebungsverfahren (näheres dazu siehe unten) kommen jedoch nur recht schleppend voran. In anderen Bereichen (Datenverarbeitung im Zivilprozeßverfahren, im Grundbuchverfahren etc.) sind noch überhaupt keine Gesetzgebungsaktivitäten zu beobachten.

Diese Sachlage verstärkt die Bedeutung des allgemeinen Datenschutzrechts (des Landesdatenschutzgesetzes) und läßt eine datenschutzgerechte Novellierung dieses Gesetzes um so dringlicher erscheinen (zu den hier bestehenden Defiziten vgl. oben Tz. 2.2).

7.2 Zivilgerichtsbarkeit

7.2.1 Automatisierung des Mahnbescheidwesens

Die grundsätzlichen Voraussetzungen und Planungen in diesem Bereich wurden im 11. Tätigkeitsbericht dargestellt (Tz. 7.2.1, S. 27 f).

Zwischenzeitlich ist eine Landesverordnung über die Einführung der maschinellen Bearbeitung des Mahnverfahrens erlassen worden (vom 5. Juli 1988, GVBl. S. 151; die maßgebliche Verordnungsermächtigung ist insoweit § 689 Abs. 3 Satz 1 sowie § 703 c Abs. 3 erster Halbsatz der Zivilprozeßordnung). Wesentlicher Inhalt dieser Verordnung ist, daß ab 1. Oktober 1988 die

automatisierte Bearbeitung der Mahnverfahren beim Amtsgericht Mayen zentral für die Amtsgerichtsbezirke Koblenz und Mayen durchgeführt wird. Der Zuständigkeitsbereich dieser zentralen Stelle ist zwischenzeitlich auf den Bezirk des Landgerichts Koblenz und des Amtsgerichts Alzey erweitert worden.

Das JM hat (im September 1988) eine Informationsschrift mit dem Titel „Das maschinelle gerichtliche Mahnverfahren – MAGM" herausgegeben, in der das Verfahren für die betroffenen Rechtsanwender detailliert dargestellt wird. Die DSK hat örtliche Feststellungen bzgl. dieses Verfahrens getroffen, die folgendes ergeben haben:

a) Die automatisiert gespeicherten Mahnverfahrensdaten können mit einem Recherchesystem ausgewertet werden, das es ermöglicht, eine große Zahl von gespeicherten Begriffen als Suchkriterien zu nutzen und Auswertungen vorzunehmen. Die technisch gegebenen Auswertungsmöglichkeiten waren nach Auffassung der DSK zu vielfältig. Beispielsweise ließen sich damit Listen erstellen mit allen Verfahren, deren Streitwert eine bestimmte Grenze überschreitet. Es ließen sich auch verschiedene Auswahlmerkmale koppeln, so daß regional durch die Person des Antragstellers oder Antraggegners eingegrenzte Auswertungen möglich waren. Die damit zu gewinnenden Informationen könnten äußerst sensibel sein, insbesondere, wenn das automatisierte Mahnverfahren flächendeckend eingesetzt wird. Die DSK hat gefordert, diese Auswertungsmöglichkeiten grundsätzlich unter dem Gesichtspunkt der Erforderlichkeit einzuschränken. Als vorrangig hat sie folgende Forderungen erhoben:

   – verfahrensübergreifende Listenerstellungen (die nicht nur dazu dienen, Informationen über ein einzelnes bestimmtes Verfahren zu erhalten) sollten von einer gesondert zu vergebenden Berechtigung abhängen und gesondert automatisiert protokolliert werden;

   – bestimmte Auswertungsmerkmale, die die unmittelbare Sachbearbeitung nicht betreffen – insbesondere die Streitwertangabe – sollten aus den zulässigen und möglichen Suchkriterien herausgenommen werden;

   – ein landesweiter umfassender Zugriff und damit lückenlose Überblicke mit personenbezogenen Daten in Listenform über bestimmte Verfahrensbereiche sollten nicht möglich sein. Dies sollte durch abgegrenzte Zugriffsberechtigungen für die Systemnutzer technisch abgesichert werden.

   Bezüglich dieser Anforderungen wurde mit dem JM Übereinstimmung erzielt.

b) Ein grundsätzlich bedeutsames Problem hat sich noch im Zusammenhang mit dem landesweiten Einsatz des automatisierten Mahnbescheidverfahrens gestellt, das nur aufgrund einer Änderung der Zivilprozeßordnung gelöst werden könnte: Angesichts der technisch möglichen Auswertungen könnten sich bei landesweitem Einsatz dieses Verfahrens Wünsche anderer öffentlicher Stellen darauf richten, zu ihrer eigenen Aufgabenerfüllung diese Auswertungen zu nutzen (wenn beispielsweise Vollstreckungsstellen der Finanzämter nach § 93 Abgabenordnung die Aufforderung an die zentrale Mahnabteilung richten, zu überprüfen, ob ein bestimmter Steuerschuldner im Zusammenhang mit Mahnverfahren als Gläubiger auftritt und damit verwertbare Forderungen gepfändet werden könnten). Eine solche Nutzungsmöglichkeit des zentralisierten Mahnbescheidwesens würde verfassungsrechtlich begründeten datenschutzrechtlichen Zielvorstellungen widersprechen, auch wenn diese Nutzung nach der derzeitigen Gesetzeslage möglicherweise zulässig wäre. Allein aufgrund der Einführung der Automation im Bereich des Mahnbescheidverfahrens sollten nach Auffassung der DSK nicht staatliche Zugriffsmöglichkeiten eröffnet werden, die eine neue Qualität besitzen, in der Vergangenheit unmöglich waren und zur zweckändernden Verwendung von Daten führen. Dies ließe sich allerdings nur durch eine ausdrückliche Zweckbindung von Mahnbescheidsdaten herbeiführen, die entweder im Landesdatenschutzgesetz oder – besser noch – auf Ebene der Zivilprozeßordnung Ausdruck finden müßte.

   Die zuletzt genannte Frage wird zur Zeit mit den Datenschutzbeauftragten des Bundes und der Länder erörtert.

7.2.2 Anordnung über Mitteilungen in Zivilsachen

Die DSK hat in der Vergangenheit wiederholt auf die datenschutzrechtliche Problematik hingewiesen, die darin liegt, daß die Zivilgerichte über das Ergebnis von Gerichtsverfahren an andere Stellen Informationen weitergeben, ohne daß dies gesetzlich geregelt ist und ohne daß die bislang in einer Verwaltungsvorschrift (der bundeseinheitlichen „Anordnung über Mitteilungen in Zivilsachen" – MiZi –) vorgesehenen Datenübermittlungen auf das erforderliche Maß beschränkt sind. Bereits 1983 (9. Tätigkeitsbericht, Tz. 8.5), dann 1985 (10. Tätigkeitsbericht, Tz. 6.10) und 1987 (11. Tätigkeitsbericht, Tz. 7.2.2) hat sie – in Übereinstimmung mit den Datenschutzbeauftragten des Bundes und der Länder – Forderungen nach einer grundlegenden Neuordnung dieses Bereichs erhoben. Die optimistische Einschätzung der DSK in ihrem 11. Tätigkeitsbericht, daß „in naher Zukunft eine gesetzliche Grundlage" für entsprechende Übermittlungen geschaffen würde, hat sich leider nicht bestätigt. Der seinerzeit vorgelegte Referentenentwurf für ein Justizmitteilungsgesetz hat dieses Stadium noch nicht verlassen. Es ist zur Zeit auch nicht absehbar, ob und mit welchem Ergebnis das Gesetzgebungsvorhaben weiterbetrieben wird.

Die DSK ist der Auffassung, daß verstärkt Anstrengungen unternommen werden sollten, um dessen Fortgang zu fördern.

7.2.3 Datenübermittlungen zwischen Gerichten

Die DSK besitzt keine Zuständigkeit, um unmittelbar das Verhalten von Gerichten im Bereich der Rechtsprechung im Zusammenhang mit der Speicherung, Übermittlung und Nutzung von Daten zu untersuchen und zu beurteilen. Dem steht die richterliche Unabhängigkeit entgegen, ein Grundsatz, der in § 24 Abs. 1 LDatG Ausdruck gefunden hat.

Dennoch hat die DSK auch in diesem Bereich durchaus die Befugnis, unabhängig von konkreten Einzelfällen allgemein zu datenschutzrechtlichen Fragen Stellung zu nehmen. Dies hat sie im Zusammenhang mit der Übermittlung von Prozeßakten von den Arbeitsgerichten an die Sozialgerichte auf Ersuchen des JM getan. Hintergrund dieser Stellungnahme ist die tatsächliche Übung der Sozialgerichte, in Streitigkeiten der verschiedensten Art, denen die Auflösung eines Arbeitsverhältnisses zugrunde liegt (etwa um Zahlung von Arbeitslosengeld), die vollständigen Arbeitsgerichtsakten anzufordern, die im vorangegangenen Arbeitsgerichtsverfahren entstanden sind. Ein Arbeitsgericht im Land Rheinland-Pfalz hat diese Verfahrensweise aus datenschutzrechtlichen Gründen in Frage gestellt und das aktenanfordernde Sozialgericht gebeten, nähere Angaben zu den Gründen der Aktenanforderung bzw. zum interessierenden Sachthema zu machen, damit ggf. Teile der arbeitsgerichtlichen Prozeßakten oder ganze Beiakten von der Übersendung ausgenommen werden könnten, die mit dem das Sozialgericht interessierenden Thema nichts zu tun haben.

Das JM hat die Auffassung vertreten, daß ein derartiges Verlangen in der Praxis zu unüberwindbaren Schwierigkeiten führen müßte, und zudem die Entscheidungskompetenz auf das Arbeitsgericht verlagert würde, ohne daß dies rechtlich geboten wäre. Die DSK hat demgegenüber betont, daß das Anliegen des betroffenen Arbeitsgerichts im Grundsatz mit den Prinzipien übereinstimmt, die die DSK seit langem vertritt (vgl. 10. Tätigkeitsbericht, Tz. 7.2.1). Sie hat jedoch gleichzeitig darauf hingewiesen, daß eine detaillierte Prüfung des Anliegens des anfordernden Sozialgerichts durch das Arbeitsgericht sicherlich nicht möglich ist. Eine – wenn auch grobe – Plausibilitätsprüfung durch das aktenübersendende Gericht, die es ermöglicht, erkennbar vom Erkenntnisinteresse des anfordernden Gerichts nicht umfaßte Aktenteile von der Aktenübersendung auszunehmen, sei aus datenschutzrechtlicher Sicht jedoch unabdingbar. Es bleibt abzuwarten, welche Verfahrensweise insofern verbindlich vorgeschrieben wird.

7.3 Strafjustiz

7.3.1 Vorbemerkung

Schwerpunkt der Tätigkeit der DSK im Bereich der Strafjustiz ist zum einen die Datenschutzkontrolle bei automatisierten Verfahren von Staatsanwaltschaften, zum anderen eine beratende Begleitung der gesetzgeberischen Aktivitäten, die sich im Bereich der Strafjustiz leider ausschließlich auf die Vorlage von neuen Referentenentwürfen zur StPO beschränkt haben (und beispielsweise nicht den Bereich des Justizmitteilungsgesetzes betroffen haben). Daneben hat die Erörterung von Kompetenzfragen eine gewichtige Rolle gespielt (siehe dazu Tz. 7.3.2).

7.3.2 Zuständigkeit der DSK in staatsanwaltschaftlichen Ermittlungsverfahren

Wie oben ausgeführt, hat die DSK im Bereich der rechtsprechenden gerichtlichen Tätigkeit keine Befugnisse. An der richterlichen Unabhängigkeit nehmen jedoch die Staatsanwaltschaften nicht teil, so daß die DSK insoweit die umfassende Prüfkompetenz in Anspruch nimmt, die ihr gegenüber allen anderen Behörden und öffentlichen Stellen des Landes zusteht (§§ 17,20 LDatG). In diesem Zusammenhang hat sich eine grundsätzliche Meinungsverschiedenheit mit dem JM an der Frage entzündet, in welchem Umfang die DSK datenschutzrechtliche Fragen überprüfen darf, die bei einem laufenden Ermittlungsverfahren auftreten. Hier haben die Generalstaatsanwälte und das Justizministerium insbesondere befürchtet, daß unter einer parallelen Kontrolltätigkeit die Effizenz der staatsanwaltlichen Arbeit Schaden erleiden könnte. Hinzu komme, daß die DSK grundsätzlich nur Befugnisse in Anspruch nehmen könne und Aufgaben besitze, wenn personenbezogene Daten in automatisierter Form verarbeitet würden. Soweit Beschwerden sich beispielsweise auf die Unzulässigkeit von Ermittlungshandlungen (insbesondere Vernehmungen etc.) bezögen, sei die DSK nicht zuständig.

Schon bezüglich dieser Grundsatzfrage vertritt die DSK eine andere Auffassung: Ihr ist nach dem Gesetz die Überwachung aller datenschutzrechtlichen Vorschriften zugewiesen (§ 17 Abs. 1 LDatG). Wenn datenschutzrechtliche Vorschriften außerhalb des Landesdatenschutzgesetzes nicht auf die automatisierte Datenverarbeitung abstellen, dann erstreckt sich nach Auffassung der DSK ihre Aufgabe auch darauf, die Einhaltung dieser Vorschriften in vollem Umfang zu kontrollieren. Unabhängig davon ist sie der Auffassung, daß insbesondere bei polizeilichen Ermittlungen regelmäßig eine automatisierte Speicherung im Gefolge der Ermittlungshandlungen erfolgt (sei es in POLIS, dem umfassenden polizeilichen Informationssystem, oder in einem POLDOK, einem ad hoc für besonders umfangreiche Verfahren eingerichteten polizeilichen Dokumentationssystem); künftig, bei Einsatz weiterer automatisierter Verfahren im Ermittlungsbereich der Polizei (vgl. dazu Tz. 5.2.1) werden entsprechende automatisierte Speicherungen noch verstärkt erfolgen.

Die hier aufgetretenen grundsätzlichen Streitpunkte wurden unter persönlicher Beteiligung des Justizministers erörtert. Es war möglich, eine praktische Verfahrensweise zu vereinbaren, die es unter Ausklammerung der gegensätzlichen Standpunkte ermöglichen dürfte, daß die DSK in ausreichendem Umfang tätig werden kann. Danach werden Datenerhebungen und Speicherungen, die im Zusammenhang mit automatisierten DV-Verfahren stehen, in vollem Umfang durch die DSK überprüft, auch wenn es sich um laufende Ermittlungsverfahren handelt; falls ein Bezug zur automatisierten Datenverarbeitung nicht oder noch nicht besteht, wird die DSK sich darauf beschränken, in entsprechenden Fällen eine Anfrage an die zuständige Aufsichtsbehörde zu richten. Sie wird dann aufgrund der erfolgenden Auskünfte ihre datenschutzrechtliche Beurteilung treffen.

Die DSK hat sich vorbehalten, von dieser Vereinbarung Abstand zu nehmen, wenn sich in der Praxis Schwierigkeiten bei der Umsetzung dieses Kompromisses zeigen sollten, die eine effektive Wahrnehmung ihres gesetzlichen Kontrollauftrags unangemessen erschweren.

7.3.3 Automatisierungsbestrebungen im Bereich der Staatsanwaltschaften

7.3.3.1 Geschäftsstellenautomation der Staatsanwaltschaften (GAST)

Die maßgeblichen organisatorischen und quantitativen Bedingungen, unter denen die Staatsanwaltschaften ihre Ermittlungstätigkeiten durchführen, und die daraus resultierenden Automatisierungszwänge wurden im 11. Tätigkeitsbericht (Tz. 7.3.1 a, S. 29 f) dargestellt. Die DSK hat dabei auch erste datenschutzrechtliche Fragen bezüglich des Einsatzes des Geschäftsstellenautomationssystemes, das von Schleswig-Holstein übernommen und in Rheinland-Pfalz bei zwei Staatsanwaltschaften, in Mainz und Zweibrücken, eingesetzt wird, formuliert. Im Berichtszeitraum hat sie örtliche Feststellungen in diesem Bereich durchgeführt, die zu folgenden Anregungen aus datenschutzrechtlicher Sicht geführt haben:

Zunächst hat die DSK darauf hingewiesen, daß es angesichts der verfassungsrechtlich gebotenen Wertung der automatisierten Speicherung personenbezogener Daten durch öffentliche Stellen als „Informationseingriffe" bedenklich ist, wenn im Strafverfolgungsbereich personenbezogene Daten automatisiert gespeichert werden, ohne daß eine bereichsspezifische gesetzliche Grundlage dafür vorhanden ist. Die DSK hat in diesem Zusammenhang insbesondere auch auf das Urteil des OLG Frankfurt vom 14. Juli 1988, Az: 3 VAs 4/88, hingewiesen, das sogar für die manuelle Dateispeicherung von Strafverfahrensdaten eine ausdrückliche gesetzliche Grundlage fordert.

Bezüglich des eingesetzten Geschäftsstellenautomationssystems GAST hat sie auf der Grundlage konkreter Feststellungen zu mehreren Fragen Stellung genommen. So erscheint ihr die Speicherungsdauer bezüglich einiger gespeicherter Daten nicht ausreichend am Erforderlichkeitsgrundsatz orientiert. Sie hat entsprechend verkürzte Löschungsfristen angeregt.

Dem zur Zeit technisch möglichen und tatsächlich genutzten Online-Lesezugriff zwischen den Staatsanwaltschaften Mainz und Zweibrücken auf die jeweiligen Strafverfahrensdaten fehlt es nach Ansicht der DSK an einer gesetzlichen Grundlage (vgl. insoweit auch unten Tz. 7.3.3.2).

Verbesserungen des Paßwortverfahrens wurden vorgeschlagen. Die DSK forderte außerdem, den Schreib- und Lesezugriff unter dem Gesichtspunkt des Erforderlichkeitsprinzips erheblich zu beschränken und dabei unmittelbar an die Zuständigkeiten der jeweils betroffenen Sachbearbeiter anzuknüpfen. In diesem Zusammenhang hat die DSK auch gerügt, daß das Datenänderungsverfahren den Datensicherungsanforderungen nicht ausreichend entspricht.

Weitere Empfehlungen betrafen die Kontrolle von Ausdrucken sowie die Erstellung einer Dienstanweisung.

Inhaltlich konnte mit dem Justizministerium weitgehend Übereinstimmung erzielt werden. Die praktische Umsetzung der Empfehlungen der DSK ist jedoch deshalb auf Schwierigkeiten gestoßen, weil das Justizministerium eine völlige Neukonzeption der Geschäftsstellenautomation der Staatsanwaltschaften – unabhängig von dem zur Zeit eingesetzten „GAST-System" – plant. Es sei wirtschaftlich unvertretbar, so lautet der Vortrag des Justizministeriums, Änderungen an einem System durchzuführen, das nur noch für eine Übergangszeit (etwa zwei Jahre) genutzt werden könne. Es müsse bis zu seiner völligen Ersetzung unverändert eingesetzt werden.

Die DSK hat jedoch demgegenüber darauf hingewiesen, daß es kaum hinnehmbar ist, ohne Beseitigung zumindest der bedeutsamsten Mängel das System unverändert weiterzuführen, zumal eine datenschutzgerechtere Lösung erst zu einem Zeitpunkt eingeführt werden dürfte, der nicht genau zu fixieren ist und der jedenfalls nicht in näherer Zukunft liegen wird.

Sie hat deshalb als ihre wichtigsten Forderungen betont:

– Beseitigung der Online-Zugriffsmöglichkeit der Staatsanwaltschaften Mainz und Zweibrücken auf die jeweils der anderen Staatsanwaltschaft zugehörigen Daten,

– Verbesserung des Paßwortverfahrens,

– Einführung einer angemessenen Speicherkontrolle.

Die Erörterungen zu diesem Punkt mit dem JM dauern an.

7.3.3.2 Aufbau eines länderübergreifenden staatsanwaltschaftlichen Informationssystems zwischen Hessen und Rheinland-Pfalz

Mitte 1988 hatten die Justizminister der Länder Hessen und Rheinland-Pfalz geplant, ein Direktzugriffsverfahren zwischen den Staatsanwaltschaften Mainz – Wiesbaden – Frankfurt und Frankenthal – Darmstadt für die jeweiligen automatisiert gespeicherten Geschäftsstellendaten einzurichten. Die beteiligten Staatsanwaltschaften sollten untereinander jeweils auf den gesamten automatisiert gespeicherten Datenbestand zugreifen können. Nähere Regelungen sollten jedoch auf Ebene einer Dienstanweisung erfolgen, die einige Einschränkungen für die Zugriffsbefugnis enthalten sollte.

Die DSK hat zwar akzeptiert, daß ein entsprechendes Verfahren zur Vereinfachung und Effektivierung der Arbeit der beteiligten Staatsanwaltschaften beitragen könnte. Dennoch mußte sie darauf hinweisen, daß auf der Grundlage des geltenden Rechts (insbesondere §§ 160, 161 StPO und § 3 Abs. 2 Nr. 2 LDatG) entsprechende Online-Datenübermittlungen nicht zulässig sind. Voraussetzung entsprechender Informationssysteme ist grundsätzlich eine Regelung in der Strafprozeßordnung (die in den vorliegenden Entwürfen zur Ergänzug der StPO auch vorgesehen ist).

Nach längerer Diskussion hat sich das JM dieser Auffassung der DSK angeschlossen, von einer Fortführung dieses Projekts wurde abgesehen (vgl. zu länderübergreifenden staatsanwaltschaftlichen Informationssystemen auch Tz. 7.3.1 b des 11. Tätigkeitsberichts).

7.3.3.3 Die Nutzung von Personalcomputern durch Staatsanwälte

Auch unabhängig vom staatsanwaltschaftlichen Computereinsatz bei den Zentralstellen für Wirtschaftsstrafsachen bzw. bei der Landeszentralstelle für Wein- und Lebensmittelstrafsachen (siehe dazu 11. Tätigkeitsbericht, Tz. 7.3.2 c, aa, bb) hat die Nutzung von Personalcomputern durch Staatsanwälte zugenommen. Hierbei kommen häufig private Geräte zum Einsatz, da die Arbeitserleichterungen, die die moderne Technik bietet, eine größere Zahl von Justizbediensteten (nicht nur Staatsanwälte, sondern auch Richter) dazu veranlaßt, auf private Kosten entsprechende Geräte zu beschaffen und zu dienstlichen Zwecken zu nutzen.

Datenschutzrechtliche Vorgaben können sich sicherlich nicht darauf beschränken, den Einsatz dienstlicher Geräte zu reglementieren und die damit verbundenen Persönlichkeitsgefährdungen durch technisch-organisatorische Maßnahmen aufzufangen, gleiche Gesichtspunkte aber beim dienstlichen Einsatz privater Geräte völlig außer Betracht zu lassen. Dementsprechend hat die DSK darauf hingewirkt, daß in den Dienstanweisungen über Datenschutz und Datensicherung bei den Staatsanwaltschaften im Lande Anforderungen an diesen PC-Einsatz aufgenommen werden. Dort ist nahezu gleichlautend folgende Regelung enthalten:

„Der dienstliche Einsatz privater Datenverarbeitungsgeräte ist nur zulässig, wenn der Dienststellenleiter darüber informiert wurde und dieser den Einsatz genehmigt hat. Die Genehmigung wird nur erteilt, wenn die betroffenen Bediensteten ihr Einverständnis dahingehend abgeben, daß das Datenverarbeitungsgerät unter den gleichen Bedingungen wie dienstliche Geräte kontrolliert werden kann, und wenn den Belangen des Datenschutzes durch die Einhaltung technisch-organisatorischer Datensicherungsanforderungen Rechnung getragen wird."

Die DSK hält entsprechende Regelungen für unabdingbar, um die eingangs geschilderte Gefahr eines „abgestuften" Datenschutzes je nach Eigentumsverhältnissen an den eingesetzten DV-Geräten zu vermindern.

Zu datenschutzrechtlichen Problemen im Zusammenhang mit Ermittlungsverfahren, die von der Polizei (auch in ihrer Eigenschaft als Hilfsbeamte der Staatsanwaltschaft) durchgeführt werden, siehe Tz. 5.2.1. In diesem Bereich ist – unabhängig davon, daß die Staatsanwaltschaft Weisungsbefugnisse gegenüber der Polizei hat – als speichernde Stelle die Polizei anzusehen. Insofern finden auch die allgemeinen Grundsätze über polizeiliche Datenverarbeitung Anwendung. Hier auftretende datenschutzrechtliche Probleme werden deshalb unter der Überschrift „Datenschutz im Polizeibereich" abgehandelt.

7.3.4 Novellierung der Strafprozeßordnung

Im Berichtszeitraum sind erneut Referentenentwürfe zur Änderung und Ergänzung des Strafverfahrensrechts unter datenschutzrechtlichen Gesichtspunkten vorgelegt worden. Eine erste umfassende Vorlage des Bundesministeriums der Justiz

datiert vom November 1988, ergänzt im Dezember 1988. Diese Vorlage ist durch einen Entwurf vom Juni 1989 (der sich inhaltlich nur an relativ wenigen Punkten vom ersten Entwurf unterscheidet) ersetzt worden. Diese Papiere (betroffen sind jeweils etwa 40 Gesetzesparagraphen, die zum Teil sehr umfangreich sind und einen äußerst komplexen Inhalt haben) wurden durch einen gemeinsamen Arbeitskreis der zuständigen Referenten der Datenschutzbeauftragten des Bundes und der Länder beraten. Nach dieser Abstimmung mit den Landesbeauftragten für den Datenschutz hat der Bundesbeauftragte für den Datenschutz inhaltlich umfassend und eingehend Stellung genommen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der DSK Rheinland-Pfalz hat zu den datenschutzrechtlichen Grundsatzfragen im Zusammenhang mit der StPO-Novellierung einen Beschluß gefaßt, der im Anhang (als Anlage 4) abgedruckt ist. Die DSK hat diesem Beschluß zugestimmt.

Sie würde es begrüßen, wenn ein Abschluß der gesetzgeberischen Tätigkeit in diesem Zusammenhang unter Berücksichtigung der aus Sicht des Datenschutzes gegebenen Empfehlungen in der näheren Zukunft erfolgen könnte.

7.3.5 Anordnungen über Mitteilungen in Strafsachen (MiStra)

Die DSK hatte bereits im 7. Tätigkeitsbericht (im Jahr 1980) auf die gesetzgeberische Verantwortung in diesem Bereich hingewiesen. Diesen Hinweis hat sie seitdem in verschiedenen Tätigkeitsberichten wiederholt (10. Tätigkeitsbericht, Tz. 6.9; 11. Tätigkeitsbericht, Tz. 7.3.3).

Da auch bezüglich der Mitteilungen in Strafsachen eine Rechtsgrundlage in dem oben bereits genannten „Justizmitteilungsgesetz" (siehe oben Tz. 2.2) geschaffen werden soll, gilt auch diesbezüglich das oben Gesagte zum Stand des Gesetzgebungsverfahrens.

Als vordringlich regelungsbedürftig hatte die DSK wiederholt das „Rückmeldungsverfahren" zwischen Polizei und Staatsanwaltschaft angesprochen (zu einem vergleichbaren bislang ungelösten Problembereich im Verhältnis zwischen Polizei und Militärstrafgerichtsbarkeit von Natostaaten vgl. 11. Tätigkeitsbericht, Tz. 4.3 d). Eine den datenschutzrechtlichen Anforderungen (vgl. zu diesen Anforderungen Anlage 3 zum 11. Tätigkeitsbericht, S. 91 f) entsprechende Regelung wurde in Rheinland-Pfalz jedoch bislang leider nicht getroffen. In der Praxis haben sich gerade an diesem Punkt erneut Unzuträglichkeiten gezeigt, die der DSK aufgrund von Eingaben bekannt geworden sind (vgl. hierzu auch Tz. 5.10).

So mußte wiederholt festgestellt werden, daß das polizeiliche Informationssystem „POLIS" unrichtige Daten gespeichert hatte, daß gebotene Löschungen unterblieben sind, weil eine Rückmeldung durch die Staatsanwaltschaft an die zuständige Polizeidienststelle über das Ergebnis des abgeschlossenen Strafverfahrens (das in diesen Fällen mit Freispruch geendet hatte) nicht erfolgt ist oder eine erfolgte Mitteilung nicht zutreffend ausgewertet wurde. Angesichts der belastenden Wirkungen von derartigen POLIS-Speicherungen (die im landesweiten Zugriff stehen und die im Einzelfall gravierende negative Auswirkungen haben können) wiederholt die DSK ihre dringende Aufforderung, die datenschutzrechtlichen Anforderungen in diesem Bereich umzusetzen und ihre praktische Einhaltung durch wirksame interne Kontrollmechanismen zu garantieren. Hierbei könnte etwa an Stichprobenkontrollen sowohl im Bereich der Staatsanwaltschaft wie im Bereich der Polizei durch die zuständigen Aufsichtsorgane (Generalstaatsanwaltschaften, Bezirksregierung/ISM) gedacht werden.

7.3.6 Datenerhebungen und Datenspeicherungen im Zusammenhang mit sog. „Ärzteverfahren"

Die Zahl der staatsanwaltschaftlichen Ermittlungsverfahren gegen Ärzte wegen betrügerischer Abrechnungen o. ä. hat erheblich zugenommen. Laut Auskunft des Ministers der Justiz vom 20. Januar 1989 (Plenarprotokoll der 43. Sitzung der 11. Wahlperiode S. 2997) wurden seit etwa 1984 316 Ermittlungsverfahren gegen Ärzte, Zahnärzte und Apotheker wegen Abrechnungsmanipulationen anhängig. Sie richteten sich gegen 367 Personen (289 Ärzte und Zahnärzte, 78 Apotheker).
Regelmäßig dann, wenn Ärzte und Zahnärzte von entsprechenden Verfahren betroffen sind, geht das staatsanwaltschaftliche bzw. polizeiliche Ermittlungsverfahren mit der Beschlagnahme von Patientenkarteien einher. Hierzu hatte die DSK aus aktuellem Anlaß bereits im Mai 1986 gegenüber der Presse folgendes erklärt:

„Gerade bei der Durchführung von Ermittlungsmaßnahmen im ärztlichen Bereich ist das Verhältnismäßigkeitsprinzip zu beachten. Das hochrangige Ziel, unkorrekte Abrechnungen im Arztbereich strafrechtlich zu verfolgen, darf nicht zu größeren Beeinträchtigungen der Patienten führen, als unabdingbar erforderlich.
Das verfassungskräftige Gebot der Verhältnismäßigkeit erfordert es, die Patientendaten so zu behandeln, daß die Belange der Betroffenen möglichst wenig beeinträchtigt werden. Dazu gehört, daß Patientenkarteien nur solange wie unbedingt nötig aus der Verfügungsbefugnis des Arztes entfernt bleiben. Außerdem muß gewährleistet werden, daß auch bei Zeugenvernehmungen das sog. „therapeutische Privileg" beachtet wird. Dies bedeutet, daß der Patient nicht durch Informationen über seinen Gesundheitszustand gefährdet werden darf. Möglicherweise ist auch die Hinzuziehung eines Arztes zur Vernehmung geboten (vergleichbar der Regelung, wonach eine Frau nur durch einen Arzt körperlich untersucht werden darf, § 81 d StPO)."

Im Zusammenhang mit dem Ermittlungsverfahren gegen ein Neuwieder Arztehepaar, das die Öffentlichkeit erheblich beschäftigte, hat die DSK örtliche Feststellungen bei der zuständigen Polizeidienststelle durchgeführt. Von betroffenen Patientinnen war gerügt worden, daß der Verhältnismäßigkeitsgrundsatz verletzt worden sei, da eine zu große Zahl polizeilicher Dienststellen zu umfangreiche Informationen unter Hinzuziehung außenstehender Personen in unangemessener Form erhoben und verwertet habe. Außerdem sei zweifelhaft, ob die Zahl der gefertigten Kopien und die Art der Anfertigung der Kopien (möglicherweise durch externe Stellen) den datenschutzrechtlichen Anforderungen genügte.

Die örtlichen Feststellungen sollten dazu dienen, diese Fragen zu klären. Der Umfang der zunächst beschlagnahmten, dann kopierten und im Original an den betroffenen Arzt zurückgegebenen Patientenunterlagen war erheblich. Insgesamt waren ca. 10 000 Patientenkarteikarten betroffen. Es wurde allerdings festgestellt, daß sowohl die Art und Weise der Fertigung der Kopien (durch Polizeibeamte) wie die weitere Behandlung (Aufbewahrung innerhalb der zuständigen Polizeidienststelle) keinen Anlaß zur Beanstandung gaben. Bezüglich des Umfanges der Beschlagnahme hat die DSK jedoch unter dem Gesichtspunkt des Verhältnismäßigkeitsgebots Bedenken geäußert. Diese werden dadurch bestärkt, daß in vergleichbaren Verfahren regelmäßig nur Karteikarten aufgrund einer Stichprobenauswahl beschlagnahmt werden. Diese Verfahrensweise wird zur Zeit durch den BGH in einem Revisionsverfahren auf seine Zulässigkeit überprüft.

Soweit die Umstände sowie Art und Ausmaß der Vernehmungen noch nachvollziehbar waren, konnten keine Verstöße gegen datenschutzrechtliche Vorgaben (hier also gegen das Verhältnismäßigkeitsgebot im Zusammenhang mit der Beeinträchtigung des informationellen Selbstbestimmungsrechts der betroffenen Zeuginnen) festgestellt werden.

Im Zusammenhang mit dem Ermittlungsverfahren wegen Kassenbetruges wurde zusätzlich ein Verfahren wegen Verstoßes gegen § 218 StGB gegen die Ärzte eingeleitet. Auch in diesem Zusammenhang sind betroffene Frauen als Zeuginnen vernommen worden. Insbesondere der dabei verwandte Fragebogen für die schriftliche Befragung, den die zuständige Staatsanwaltschaft an die Zeuginnen versandt hatte, war Gegenstand ausführlicher Erörterungen in der Presse und auch im Landtag. Da insofern die aufgetretenen Fragen öffentlich erörtert worden sind (vgl. dazu die Große Anfrage der Fraktion DIE GRÜNEN, Drucksache 11/2079, und die Antwort des Ministeriums der Justiz vom 14. März 1989, Drucksache 11/2352) und in Anbetracht der Tatsache, daß der ursprünglich verwendete Fragebogen durch das JM zurückgezogen wurde und für künftige Fälle nicht mehr eingesetzt werden soll, hat die DSK keine Veranlassung mehr gesehen, ihrerseits eine inhaltliche Stellungnahme zu diesem Punkt abzugeben.

Die DSK hat jedoch das Ergebnis der örtlichen Feststellungen und insbesondere die Frage der Verhältnismäßigkeit der Beschlagnahme von Patientenkarteikarten zum Gegenstand von Erörterungen mit dem JM gemacht. Sie erwartet, daß die Sensitivität im Justizbereich beim Umgang mit entsprechenden Patientendaten auch praktisch Ausdruck findet in weiteren konkreten Maßnahmen sowohl bei der Beschränkung des Umfangs der Beschlagnahme wie in bezug auf die Aufbewahrung, den Schutz und die Nutzung der beschlagnahmten Unterlagen.

7.4 Strafvollzug

7.4.1 Novellierung des Strafvollzugsgesetzes

Die DSK hat bezüglich der datenschutzrechtlichen Ergänzung des Strafvollzugsgesetzes im 11. Tätigkeitsbericht (Tz. 7.4.2) einen Sachstandsbericht gegeben und ihre eigene Tätigkeit in diesem Zusammenhang dargestellt.

Ein Fortgang der Gesetzgebungsverfahren des Bundes war nicht festzustellen. Die im letzten Tätigkeitsbericht (a. a. O.) geäußerte Vermutung ist nahezu zur Gewißheit geworden, daß der eingetretene Stillstand dieses Verfahrens auf der grundsätzlichen Kritik beruht, die von den Landesjustizverwaltungen am Arbeitsentwurf geübt worden ist. Diese hatten insbesondere gerügt, daß die vorgesehenen Regelungen nicht praktikabel seien. Die DSK fordert das Justizministerium auf, durch konstruktive Vorschläge auch in diesem Bereich dazu beizutragen, daß den verfassungsrechtlichen Anforderungen genügt wird.

7.4.2 Forschung im Strafvollzug

7.4.2.1 Kriminologische Forschung durch den Kriminologischen Dienst des Landes Rheinland-Pfalz

§ 166 Strafvollzugsgesetz fordert die Länder auf, einen kriminologischen Dienst einzurichten, der den Vollzug wissenschaftlich fortentwickeln und die Ergebnisse der Forschung für Zwecke der Strafrechtspflege nutzbar machen soll. Damit hat der Gesetzgeber eine Vollzugsforschung vorgesehen, die als Eigen- und Auftragsforschung durch die Vollzugsverwaltung selbst wahrgenommen wird. In Rheinland-Pfalz hat dies organisatorisch dadurch Ausdruck gefunden, daß die sozialtherapeutische Anstalt JVA Ludwigshafen damit beauftragt worden ist, den kriminologischen Dienst für den Strafvollzug des Landes Rheinland-Pfalz wahrzunehmen (AV des JM vom 2. August 1988, JBl. S. 199).

Die DSK hat unter dem Gesichtspunkt, daß kriminologische Forschung in Strafvollzugsanstalten mit sensiblen Daten befaßt ist, und daß das informationelle Selbstbestimmungsrecht einsitzender Strafgefangener grundsätzlich in gleichem Umfang zu wahren ist wie das unbescholtener Bürger, örtliche Feststellungen bei der Sozialtherapeutischen Anstalt in Ludwigshafen durchgeführt, die ihre Tätigkeit als „Kriminologischer Dienst" betrafen. Wesentliche Ergebnisse waren:

- Aufgrund der relativ geringen personellen und sachlichen Ausstattung des kriminologischen Dienstes wurden in den letzten Jahren nur wenige Forschungsvorhaben durchgeführt (insgesamt 3). Die vorhandene DV-Ausstattung wird in erster Linie zur Erstellung von Texten (also als Schreibautomat) genutzt.

- Soweit datenschutzrechtliche Fragen und Bedenken aufgetreten sind, betrafen diese ein Forschungsprojekt, dessen Gegenstand die Einstellungspraxis bei Bediensteten des mittleren Justizvollzugsdienstes war. Dieses Forschungsprojekt liegt jedoch schon längere Zeit (ca. zehn Jahre) zurück, so daß eine vertiefende Behandlung unangemessen erscheint. Die DSK hat aber gegenüber der Sozialtherapeutischen Anstalt deutlich gemacht, daß die Rechte der Betroffenen auch bei solchen Forschungsvorhaben zu wahren sind und daß künftig das Selbstbestimmungsrecht der Betroffenen stärker beachtet werden muß.

7.4.2.2 Sonstige Forschung im Strafvollzugsbereich

Die DSK hatte Veranlassung, die Justizverwaltung (sowohl die betroffenen Justizvollzugsanstalten wie das JM) darauf hinzuweisen, daß bei Forschungsvorhaben in Strafvollzugsanstalten das Prinzip der Freiwilligkeit der Teilnahme ebenso streng zu beachten ist wie außerhalb von Justizvollzugsanstalten. Voraussetzung der Wirksamkeit der Zustimmung zu Datenerhebungen und Datenspeicherungen (insbesondere zu Datenspeicherungen in automatisierten Verfahren) ist es, daß die Betroffenen vor Teilnahme an der jeweiligen Erhebung ausreichend über das Projekt unterrichtet werden, damit ihre Einwilligung als „informierte Einwilligung" angesehen werden kann. Außerdem muß gesichert sein, daß die Betroffenen bei der Entscheidung über die Teilnahme keinem unzulässigen Druck ausgesetzt sind.

Schließlich ist darauf zu achten, daß die erhobenen Daten ausschließlich zu Forschungszwecken verwendet werden und nicht gleichzeitig Vollzugszwecken zugeführt werden (wenn dies nicht ebenfalls von der Einwilligung der Betroffenen mit umfaßt ist). Dabei sind verfahrensmäßige Vorkehrungen zu treffen, damit nicht Justizvollzugsbedienstete zwangsläufig Kenntnisse erhalten, die auch für Vollzugszwecke nutzbar, dafür aber nicht bestimmt sind. Diese Problematik wurde in einem Fall deutlich, in dem ein in England ansässiger Forscher Vollzugsbedienstete um ihre Mithilfe bei der Befragung von Gefangenen gebeten hat. Ursprünglich war vorgesehen, daß die Justizvollzugsbediensteten Fragebögen mit sehr sensitivem Inhalt (zu moralischen Wertvorstellungen und zur Ehrlichkeit der Gefangenen) offen einsammeln, auf Vollständigkeit der Beantwortung prüfen und dann erst an den Wissenschaftler übersenden sollten. Die DSK hat auf ein Verfahren hingewirkt, in dem eine Kenntnisnahme des Befragungsergebnisses durch die Vollzugsbediensteten ausgeschlossen war. Vergleichbare Probleme stellten sich auch in anderen Fällen.

7.4.3 Stempelaufdruck „Vorsicht Blutkontakt" auf bzw. in Gefangenengesundheitsakten

Anläßlich einer Eingabe ist die DSK darauf aufmerksam geworden, daß die Justizvollzugsanstalten in zwei Fallgruppen den Stempelaufdruck „Vorsicht Blutkontakt" auf Gesundheitsakten der Strafgefangenen angebracht haben:

- wenn ein Gefangener HIV-positiv ist

  sowie

- wenn ein Gefangener einmal an Virushepatitis B erkrankt war.

In diesem Zusammenhang war zunächst fraglich, ob entsprechende Stempelaufdrucke auf den Gefangenengesundheitsakten überhaupt zulässig sein können. Durch die auf dem Umschlag offen angebrachte Kennzeichnung kann eine Vielzahl von Personen Kenntnis von dieser Warnung erhalten, die diese zu Erfüllung ihrer Aufgaben nicht benötigen. Dieses Argument hat die Justizverwaltung akzeptiert und angeordnet, daß künftig entsprechende Kennzeichnungen nur innerhalb der Akte angebracht werden dürfen.

Zweifelhaft war außerdem, ob es gerechtfertigt ist, einmal an Hepatitis B erkrankte Gefangene in gleicher Weise aktenmäßig zu kennzeichnen wie HIV-positive Gefangene. Einige Justizvollzuganstalten haben den entsprechenden Gefangenen angeboten, auf Wunsch den Zusatz „Hepatitis B" an den fraglichen Stempelaufdruck anzufügen.

Schließlich war zu fragen, ob eine entsprechende Kennzeichnung wirklich bei allen einmal an Hepatitis B erkrankten Gefangenen gerechtfertigt ist, mit anderen Worten: Bleiben wirklich alle entsprechenden Gefangenen infektiös, oder kann die Infektiosität nicht bei einem relevanten Prozentsatz der betroffenen Personen faktisch ausgeschlossen werden?

Das OLG Koblenz sowie einige Justizvollzugsanstalten im Land vertreten die zuletzt genannte Auffassung. Dementsprechend haben diese Justizvollzugsanstalten angeordnet, daß eine entsprechende Aktenkennzeichnung nur dann erfolgt, wenn sich aufgrund von aktuellen Untersuchungsergebnissen eine Infektiosität des betreffenden Gefangenen bestätigt.

Die DSK hat sich dieser Auffassung nach Einholung von Stellungnahmen, insbesondere des Medizinaluntersuchungsamts in Koblenz, angeschlossen.

In der Folge hat sie das JM gebeten, für eine einheitliche Regelung in diesem Zusammenhang mit dem genannten Inhalt für alle Justizvollzugsanstalten des Landes Sorge zu tragen.

Das JM interpretiert die vorliegenden medizinischen Stellungnahmen zur Frage der Infektiosität ehemals an Hepatitis B erkrankter Personen anders als das OLG Koblenz, die DSK und einige Justizvollzugsanstalten und geht davon aus, daß ein Infektionsrestrisiko in jedem Fall bestehen bleibe. Es lehnt deshalb eine einheitliche Regelung für alle Justizvollzugsanstalten ab.

Die DSK vermag dies nicht zu akzeptieren. Trotz eindringlicher Hinweise auf die deutlichen medizinischen Stellungnahmen in diesem Zusammenhang war das Justizministerium nicht davon zu überzeugen, von seiner ursprünglichen Auffassung abzugehen. Die DSK bedauert, daß damit das Persönlichkeitsrecht in Gestalt des informationellen Selbstbestimmungsrechts der betroffenen Gefangenen einiger Justizvollzugsanstalten unverhältnismäßig beeinträchtigt wird, und daß damit auch weitere Rechtsstreitigkeiten (verbunden mit Kosten für das Land Rheinland-Pfalz) nicht auszuschließen sind.

7.4.4 Datenübermittlungen durch Bewährungshelfer

In verschiedenen Zusammenhängen hat sich für die DSK die Frage gestellt, in welchem Umfang Bewährungshelfer andere öffentliche und private Stellen über Verhältnisse der ihnen anvertrauten Probanden unterrichten dürfen. Unzweifelhaft ist, daß Bewährungshelfer dem zuständigen Gericht über die Lebensführung des Verurteilten und über Verstöße gegen Auflagen, Weisungen, Anerbieten und Zusagen zu berichten haben (§ 56 d Abs. 3 StGB). Außerdem können sie vor allem an Jugendämter, Arbeitsämter, Sozialhilfe- und Fürsorgebehörden, an freie Wohlfahrtsverbände und an besondere Organisationen der Straffälligenfürsorge entsprechende Informationen weitergeben, wenn dies unzweifelhaft im Interesse ihrer Probanden liegt (dies ergibt sich aus § 8 Abs. 1 des Landesgesetzes über die Bewährungshelfer vom 11. Juli 1956, BS 3216-10). Dem Begehren einer Landesnervenklinik konnte die DSK in diesem Zusammenhang jedoch nicht in vollem Umfang zustimmen: Diese Klinik war unter anderem zuständig für die Entziehungsbehandlung alkoholabhängiger Personen aus Rheinland-Pfalz, die dort nach Begehung einer Straftat zwangsweise untergebracht worden sind (§ 64 StGB). Sie wollte nun die Rückfallquote bei entlassenen Betroffenen und damit den Erfolg ihrer Arbeit überprüfen. Da die Betroffenen im Regelfall auch nach der Entlassung noch unter Führungs- bzw. Bewährungsaufsicht stehen, wäre es der einfachste Weg gewesen, wenn die zuständigen Bewährungshelfer entsprechende Informationen bzw. Berichte an die Klinik hätten weitergeben können. Bezüglich der begehrten Übermittlungen gilt jedoch die Verschwiegenheitspflicht des Bewährungshelfers (die gem. § 203 Abs. 2 Nr. 1 StGB strafbewehrt ist). Die DSK wies jedoch auf die Möglichkeit hin, daß die Gerichte im Wege einer Bewährungsauflage eine entsprechende Berichtspflicht begründen oder daß die betroffenen Bewährungshelfer die Probanden um Zustimmung zur Übermittlung entsprechender Informationen ersuchen. Dementsprechend wurde die Klinik unterrichtet.

Die DSK geht davon aus, daß auch unter diesen Voraussetzungen eine sinnvolle Erfolgskontrolle möglich ist.

7.5 Justizregister

7.5.1 Handelsregister

Im Berichtszeitraum hat eine private Firma beabsichtigt, sämtliche im Bundesgebiet in den Handelsregistern der rund 440 Registergerichte eingetragenen Firmen nach einer bestimmten Struktur automatisiert zu erfassen. Zu diesem Zweck hat dieses Unternehmen bei Gerichten beantragt, unter Einsatz eigener Hilfsmittel und eigenen Personals das gesamte Handelsregister durch Mikroverfilmung aufzunehmen. Anschließend sollten die Daten automatisiert erfaßt und aufgrund der Eintragungen im Bundesanzeiger jeweils aktualisiert werden. Die Datenbank sollte dann der Privatwirtschaft zur freien Nutzung gegen Entgelt zur Verfügung gestellt werden. Die Datenschutzbeauftragten des Bundes und der Länder haben sich mit der Frage befaßt, ob ein entsprechendes Vorhaben zulässig ist, und haben übereinstimmend dagegen Stellung genommen. Maßgebend dafür ist, daß der Bundesgesetzgeber bewußt die dezentrale Handelsregisterführung vorgesehen hat. Die geplante Form der Datennutzung würde grundsätzlich neue Auswertungsmöglichkeiten und grundsätzlich veränderte Nutzungsbedingungen schaffen. Es könnten Informationsprofile erstellt werden, die Aussagen ermöglichen, die über die Funktion des Handelsregisters, wie sie der Gesetzgeber im Auge hatte, weit hinausgehen. Eine entsprechende Veränderung in diesem Zusammenhang wäre nur durch eine eindeutige gesetzliche Regelung möglich. Dann hätte der Gesetzgeber aber zudem Datenschutzgesichtspunkte insbesondere bei Auswertung und Nutzung der dann entstehenden zentralen Datenbank zu berücksichtigen.

Die Justizverwaltungen haben sich dieser Auffassung weitgehend angeschlossen und häufig entsprechende Anträge der betroffenen Privatfirma abgelehnt. Auch der Bundesgerichtshof, der in diesem Zusammenhang angerufen wurde und die Angelegenheit am 12. Juli 1989 (Az. IV a ARZ (VZ) 9/88) entschieden hat, hat die vorgenannte Auffassung für ausreichend erachtet, um das Begehren der betroffenen Antragstellerin abzulehnen.

7.5.2 Schuldnerverzeichnis

7.5.2.1 Novellierung des § 915 ZPO

Aus welchen Gründen und in welchem Umfang gesetzgeberische Regelungsbedarf im Zusammenhang mit der Führung des Schuldnerverzeichnisses besteht, hat die DSK in ihren vergangenen Tätigkeitsberichten (vergl. 8. Tätigkeitsbericht, Tz. 5.25; 10. Tätigkeitsbericht, Tz. 6.11) wiederholt dargestellt.

Die DSK hat – auch, um die praktische Relevanz des Schuldnerverzeichnisses besser abschätzen zu können – in einer Umfrage an die Industrie- und Handelskammern des Landes in Erfahrung gebracht, in welcher Auflage die Informationen aus dem Schuldnerverzeichnis jeweils veröffentlicht werden. Folgende Tabelle gibt darüber einen Überblick:

Bezieher von Schuldnerlisten	Koblenz	Pfalz	Rheinhessen	Trier
kammerangehörig	118	2 656	478	392
auswärtig	29	144	25	8
insgesamt	147	2 800	503	400

Die Zahl der Bezieher verdeutlicht, daß der Gesetzgeber dringend Vorgaben für den Bezug dieser Schuldnerlisten formulieren sollte, da die quantitative Komponente der Problematik durchaus erheblich ist. Auch die nachstehend beschriebenen Fälle bestätigen, daß Handlungsbedarf in diesem Zusammenhang besteht.

Die gesetzgeberischen Aktivitäten sind im Berichtszeitraum leider nicht wesentlich vorangeschritten. Die DSK erwartet, daß die Landesregierung ihren Einfluß geltend macht, um die gesetzliche Situation insoweit entscheidend zu verbessern.

7.5.2.2 Mißbräuchliche Verwertung von Daten aus den Schuldnerverzeichnissen

Ein Betrugsverfahren, das Millionenschäden ahnden soll, ist in Rheinland-Pfalz anhängig. Sogenannte „Finanzmakler" haben Schuldnerverzeichnisse der Industrie- und Handelskammern (die diese für eigene und fremde Kammerangehörige veröffentlichen) bezogen, die Anschriften der Schuldner aber nicht bestimmungsgemäß genutzt, sondern die betroffenen Schuldner mit psychologisch geschickten Werbebriefen zum Abschluß von neuen Kreditverträgen zu ermuntern versucht. In Wirklichkeit wurden keine Kreditverträge abgeschlossen, es wurden den betroffenen Schuldnern zum Teil Unfall- und Lebensversicherungen – angeblich zur Vorbereitung einer Kreditvergabe – vermittelt, es wurden auch „Bearbeitungsgebühren" in Rechnung gestellt, ohne daß eine weitere Bearbeitung erfolgte. Auch in anderen Teilen des Bundesgebietes sollen „Finanzmakler" in ähnlicher Weise tätig sein.

Die mißbräuchliche Verwendung von Daten aus Schuldnerverzeichnissen zu diesen genannten Zwecken wird den betrügerisch agierenden Firmen leicht gemacht: Eine effektive Prüfung der Zuverlässigkeit der Bezieher der genannten Schuldnerlisten durch die Industrie- und Handelskammern findet nicht statt (sie kann praktisch auch kaum stattfinden). Wirksame Abhilfe kann nur in einer Beschränkung der bislang nahezu unbeschränkten Zugriffsbefugnisse privater Dritter liegen. In diesem Sinn hat die DSK gegenüber dem Bundesbeauftragten für den Datenschutz und gegenüber dem Justizministerium Stellung genommen.

7.5.2.3 Verwechslungsgefahren bei der Benutzung von Daten aus den Schuldnerverzeichnissen

Die Schuldnerdaten aus dem Schuldnerverzeichnis werden auch von Kreditauskunfteien und der „Schufa" (Schutzgemeinschaft für allgemeine Kreditsicherung) genutzt. Der DSK wurde ein Fall bekannt, wo der betroffene Beschwerdeführer bei der Schufa mit „zwei Haftbefehlen" gespeichert war, die angeblich wegen Zahlungsunfähigkeit erlassen worden waren. Bei einer Nachprüfung stellte sich heraus, daß die Schufa einer Namensverwechslung erlegen war: Bei der Auswertung einer Schuldnerliste hatte sie den Vater des Beschwerdeführers, den die fragliche Eintragung betraf, mit dem Beschwerdeführer, der den gleichen Vor- und Zunamen trägt, verwechselt. Die DSK hat in diesem Zusammenhang darauf hingewiesen, daß es unabdingbar ist, eindeutige Identifizierungen bei der Veröffentlichung bzw. Weitergabe von Schuldnerdaten zu ermöglichen. Zu diesem Zweck ist aber neben Name und – möglicherweise – Anschrift jedenfalls die Angabe des Geburtsdatums erforderlich. Bei einem Teil der Daten aus dem Schuldnerverzeichnis erfolgt dies bereits; ohne nach Auffassung der DSK nachvollziehbare sachliche Gründe wird hier jedoch differenziert und das Geburtsdatum nicht durchgängig aus dem gerichtlichen Schuldnerregister an die Industrie- und Handelskammern und sonstige Adressaten übermittelt. Die DSK hat in diesem Zusammenhang gegenüber dem Justizministerium eine Veränderung empfohlen. Ein Ergebnis ihrer Bemühungen ist z. Z. noch nicht absehbar.

7.5.2.4 Einrichtung eines zentralen Schuldnerregisters durch eine private Firma

Vergleichbar der Errichtung eines zentralen Handelsregisters beabsichtigt eine private Firma, ein zentrales Schuldnerregister einzurichten und zunächst allen Rechtsanwälten in der Bundesrepublik die Nutzung gegen Entgelt anzubieten.

Aus den gleichen Überlegungen, die oben im Zusammenhang mit der zentralen Errichtung eines Handelsregisters angesprochen worden sind, hat die DSK Bedenken gegen die Zulässigkeit einer zentralen Registrierung. Es kommt hinzu, daß Schuldnerdaten erheblich sensitiver sind als Angaben, die dem Handelsregister entnommen werden können. Die DSK wird sich dafür einsetzen, daß dieses Vorhaben zunächst eingestellt wird und daß es nur aufgrund gesetzlicher Vorgaben weiterbetrieben wird, die die Interessen aller von einem derartigen Verfahren Betroffenen angemessen berücksichtigen.

7.6 Genomanalyse und informationelle Selbstbestimmung

Aufgrund des Abschlußberichts der Enquête-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Bundestagsdrucksache 10/6775) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Beschluß gefaßt über datenschutzrechtliche Aspekte dieser neuen wissenschaftlichen Erkenntnismöglichkeiten (der Beschluß ist als Anlage 5 abgedruckt).

Die Landesregierung hat sich in diesem Zusammenhang schon frühzeitig stark engagiert und durch den Einsatz der „Bioethik-Kommission" signalisiert, daß sie den rechtlichen Folgen des Einsatzes neuer Technologien im Bereich der Genetik besondere Bedeutung beimißt. Die DSK ist in diesem Zusammenhang nicht unmittelbar beteiligt worden. Sie erwartet jedoch, daß die Landesregierung auch den Überlegungen zum Datenschutz in diesem Bereich den angemessenen Stellenwert einräumt.

8 Umweltschutz

8.1 Vorbemerkung

Mit dem zunehmenden Einsatz der Datenverarbeitung zur Erfüllung von Aufgaben des Umweltschutzes wachsen auch die Datenschutzprobleme. Immer häufiger und in immer größerem Umfange werden Informationen über Art und Ausmaß von Umwelteinwirkungen sowie über Gesundheits- und Umweltgefährdungen in Akten festgehalten oder in automatisierten Verfahren gespeichert. Die Erforderlichkeit solcher Maßnahmen ist nicht zu bestreiten, soll Umweltschutz sich nicht in ebenso abstrakten wie folgenlosen Appellen erschöpfen.

Die Datenschutzprobleme sind außerordentlich vielfältig; sie beruhen zu einem erheblichen Teil auf dem Fehlen normenklarer gesetzlicher Regelungen für die Datenerhebung und Datenverarbeitung. Generalklauseln, wie sie das Landesdatenschutzgesetz enthält, sind vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts kaum noch geeignet, Informationseingriffe zu legitimieren. Ihre Anwendung verbietet sich oft auch deshalb, weil nicht die Erhebung und Verarbeitung personenbezogener Daten im Sinne von Daten natürlicher Personen in Rede steht, sondern Betriebs- und Geschäftsgeheimnisse juristischer Personen betroffen sind. Erschwerend kommt hinzu, daß Regelungszuständigkeiten sowohl vom Landesgesetzgeber, wie auch vom Bundesgesetzgeber und von den Europäischen Gemeinschaften in Anspruch genommen werden.

8.2 Wasserwirtschaft

8.2.1 Wasserwirtschaftliches Informationssystem

Einen Schwerpunkt der Datenverarbeitung im Geschäftsbereich des MUG bildet die Wasserwirtschaft. So entstand beispielsweise im Berichtszeitraum ein wasserwirtschaftliches Informationssystem, das Überwachungs- und Kontrollzwecken nach den Vorschriften des Wasserhaushaltsgesetzes, des Landeswassergesetzes und des Abwasserabgabengesetzes dient. Eine besondere Bedeutung hat dabei die Wahrnehmung eines Alarm- und Kontrolldienstes. Gespeichert werden auch die Daten von Betreibern wasserwirtschaftlicher Anlagen; soweit diese als personenbezogene Daten zu qualifizieren sind, finden die Vorschriften des Landesdatenschutzgesetzes Anwendung.

8.2.2 Automatisierte Trinkwasserdatenbank

In einer automatisierten Trinkwasserdatenbank werden die Ergebnisse der nach der Trinkwasserverordnung vorgeschriebenen Wasseruntersuchungen gespeichert. Soweit es sich um die Untersuchungsergebnisse sog. Eigenversorgungsanlagen handelt, die von natürlichen Personen betrieben werden, liegen die Anwendungsvoraussetzungen des Landesdatenschutzgesetzes vor. Da normenklare Rechtsgrundlagen für die Datenerhebung und -übermittlung insoweit nicht existieren, ist die Datenerhebung und -verarbeitung nur mit ausdrücklicher Zustimmung der Betreiber von Eigenversorgungsanlagen zulässig.

8.2.3 Einrichtung eines Landesabwasserkatasters

Angesichts der Notwendigkeit, die Anstrengungen zur Gewässerreinhaltung zu intensivieren, ist die öffentliche Hand bestrebt, Kläranlagen bestmöglich technisch auszustatten und optimal zu betreiben. Der Erfolg solcher Bemühungen ist jedoch gefährdet, wenn Schadstoffe über das unvermeidbare Maß hinaus in Kläranlagen eingeleitet werden. Es geht also darum, den Schadstoffanfall weitgehend zu reduzieren oder Schadstoffe ganz zu vermeiden.

Das MUG geht davon aus, daß diese Aufgaben nur dann zu erfüllen sind, wenn den zuständigen Behörden detaillierte Informationen über Betriebseinrichtungen, Produktionsvorgänge sowie die bei diesen Vorgängen anfallenden Stoffe zur Verfügung stehen. Es beabsichtigt, diese Informationen bei allen Schadstoffeinleitern unter Verwendung eines umfangreichen Fragebogens zu erheben, sie zu erfassen, in einem Landesabwasserkataster zu speichern und den zuständigen Behörden in dem erforderlichen Umfange zur Verfügung zu stellen.

Die datenschutzrechtliche Relevanz des Projekts liegt auf der Hand: Informationen über Betriebseinrichtungen, Produktionsvorgänge und die dabei verwendeten Stoffe sind Betriebs- und Geschäftsgeheimnisse, ihre mißbräuchliche Verwendung kann schwerwiegende Folgen haben. Mit dem Argument „Auch bei Umfragen und Erhebungen in der Wirtschaft sind Belange des Datenschutzes zu beachten" sprachen sich die Arbeitsgemeinschaft „Umweltfragen" der rheinland-pfälzischen Industrie, der Landesverband der chemischen Industrie sowie die Industrie- und Handelskammer Koblenz in öffentlichen Stellungnahmen gegen die Datenerhebung aus.

Die DSK ging bei der Beurteilung der Zulässigkeit des Projekts davon aus, daß sich aus den Vorschriften des Landeswassergesetzes, des Wasserhaushaltsgesetzes sowie aus den Richtlinien des Rates der Europäischen Gemeinschaften Zielbestimmungen und Aufgabenzuweisungen ergeben, die Interventionen im Bereich der Abwasserentstehung einschließen. Nach ihrer Auffassung besteht indessen keine Auskunftspflicht im Sinne einer mit Zwangsmitteln durchsetzbaren Rechtspflicht, sondern die Auskunftserteilung gehört zu den Obliegenheiten der Betriebe, die eine Genehmigung der Gewässerbenutzung als Direkteinleiter (§§ 7, 21 Abs. 1 und 2 Wasserhaushaltsgesetz) oder die Genehmigung der Einleitung von Stoffen in die Anlagen der öffentlichen Abwasserbeseitung als Indirekteinleiter (§§ 55 und 57 Landeswassergesetz i. V. m. der hierzu ergangenen Landesverordnung und die Allgemeinen Entwässerungssatzungen der Gemeinden) beantragen. Die Befugnis, Daten außerhalb des Genehmigungsverfahrens zu erheben, ergibt sich aus § 7 a Wasserhaushaltsgesetz, § 93 Landeswassergesetz sowie aus dem Untersuchungsgrundsatz des Verwaltungsverfahrensrechts (§ 1 Landesverwaltungsverfahrensgesetz i. V. m. § 24 Verwaltungsverfahrensgesetz des Bundes).

Die Ausgestaltung der Auskunftserteilung als Obliegenheit bedeutet, daß dem Einleiter im Falle der Auskunftsverweigerung Nachteile entstehen können, beispielsweise durch Nichterteilung einer Einleitungsgenehmigung oder dadurch, daß Einleitungsgenehmigungen widerrufen werden.

Die DSK forderte, daß die Betriebe in allen Einzelheiten über die Rechtsgrundlagen der Datenerhebung informiert werden, und daß Datenübermittlungen nur insoweit erfolgen, als sie nach den gesetzlichen Vorschriften zugelassen sind.

Die DSK bedauert, daß diese Grundsatzfragen zur Datenerhebung und -verarbeitung erst zur Klärung an sie herangetragen wurden, als die Fragebogen im Druck fertiggestellt waren. Nachdem die Kommission, dem Wunsche des Ministeriums entsprechend, ihre Stellungnahme bereits im März dieses Jahres in aller Eile vorgelegt hatte, ist offenbar nichts weiter geschehen. Das Verfahren wurde weder zum Datenschutzregister angemeldet, noch ist geklärt, welche Behörde speichernde Stelle ist, welche Verarbeitungen im einzelnen durchgeführt werden, welche Übermittlungen konkret vorgesehen sind und zu welchem Zeitpunkt die Daten gelöscht werden. Die DSK ist weiterhin um Klärung bemüht.

8.3 Naturschutz und Landschaftspflege

Im Auftrag des MUG wurde eine Vorstudie für die Entwicklung eines Landschaftsinformationssystems – LANIS RP – erstellt. Definiert wird dieses System als eine „abgrenzbare Organisationsform, die dazu dient, aufgrund von Kommunikationsprozessen naturraumbezogene Kenntnisse zweckdienlich auszutauschen".

Die Tatsache, daß wiederum nur in Ausnahmefällen personenbezogene Daten gespeichert werden sollen, darf nicht darüber hinwegtäuschen, daß das System gleichwohl von datenschutzrechtlicher Relevanz ist. Dies insbesondere deshalb, weil ein hohes Maß an vertikaler und horizontaler Integration, also ein möglichst umfassender Datenzugriff und -austausch zwischen den Behörden und innerhalb der Behörden angestrebt wird. Erfahrungsgemäß stoßen derartige Integrationsbestrebungen sehr bald an rechtliche Schranken, weil schließlich doch der Zugriff auf personenbezogene Daten, die für ganz andere Zwecke erhoben und gespeichert wurden, in Rede steht. Den Projektverantwortlichen ist zu empfehlen, dies bei ihren Planungen zu berücksichtigen. Die DSK wird die weitere Entwicklung beobachten.

8.4 Abfallwirtschaft; Aufzeichnungen über Altablagerungen von Stoffen

8.4.1 Allgemeines

Immer wieder stellt sich die Frage, ob und ggf. in welchem Umfange der Inhalt von Registern mit Aufzeichnungen über Altablagerungen von Stoffen – sog. Abfalldeponiekataster und Altlastenkataster – an andere Behörden oder private Interessenten übermittelt oder sogar veröffentlicht werden darf. Die datenschutzrechtliche Problematik ist evident: Einerseits besteht ein starkes öffentliches und privates Interesse an möglichst breiter Information über die Aufzeichnungen in solchen Katastern, das sich durchaus auch auf umweltbezogene Sachangaben in einer tiefen regionalen Gliederung beziehen kann. Andererseits kann die Offenbarung grundstücksbezogener – und damit personenbeziehbarer – Daten zu gravierenden Beeinträchtigungen schutzwürdiger Belange von Grundstückseigentümern führen.

Für die datenschutzrechtliche Beurteilung ist weiter von Bedeutung, daß die Informationen über Altlasten nur in den seltensten Fällen zuverlässig sind. Aus fachlicher Sicht wird eine Fläche mit Altablagerungen erst dann als Altlast eingestuft, wenn feststeht, daß von ihr nachweislich Gefahren für die Allgemeinheit ausgehen. Gespeichert werden aber auch Hinweisdaten und andere ungesicherte Informationen.

8.4.2 Veröffentlichung personenbeziehbarer Daten

Die DSK hat aus gegebener Veranlassung die Zulässigkeit der Veröffentlichung von Katastereintragungen geprüft. Ausgangspunkt war die Antwort der Landesregierung – Drucksache 11/1039 – auf eine Kleine Anfrage, in der um nähere Angaben zu Altablagerungen im Landkreis Neuwied gebeten wurde. Die Landesregierung wies darauf hin, daß die Erhebungsergebnisse und damit auch die näheren Angaben über die genaue Lage und Flurstücksnummer der betroffenen Grundstücke aus datenschutzrechtlichen Gründen nur den für den Vollzug des Abfallgesetzes zuständigen Behörden zur Verfügung stünden. In einer Ergänzung ihrer Antwort – Drucksache 11/1196 – bekräftigte sie ihre Auffassung mit dem Hinweis, daß sich die Altablagerungen überwiegend auf Grundstücken von Privaten befänden. Es handele sich daher bei den Angaben über die genaue Lage und die Flurstücksnummer der betroffenen Grundstücke regelmäßig um personenbezogene Daten, bei deren Weitergabe das verfassungsmäßig geschützte Recht auf informationelle Selbstbestimmung zu beachten sei. Dies sei auch bei der Beantwortung einer Kleinen Anfrage zu berücksichtigen, die der Öffentlichkeit und damit der Allgemeinheit zugänglich gemacht werde.

Die DSK stimmt dieser Rechtsauffassung im Grundsatz zu. Sofern, wovon auszugehen ist, die Altlastenkataster oder Abfalldeponiekataster in Dateiform oder in automatisierten Verfahren geführt werden, liegen die formalen Anwendungsvoraussetzungen des Landesdatenschutzgesetzes vor. Die Zulässigkeit der parzellenscharfen, also personenbeziehbaren Bekanntgabe von Informationen aus den Katastern im Rahmen der Antwort auf eine Kleine Anfrage bestimmt sich nach § 7 dieses Gesetzes, denn im Rechtssinne werden bei öffentlicher Beantwortung die Daten an Stellen außerhalb des öffentlichen Bereichs übermittelt. Aus der Anwendung dieser Vorschrift folgt, daß die Offenbarung von Daten, die in automatisierten Verfahren verarbeitet werden, in Ermangelung einer speziellen gesetzlichen Übermittlungsregelung nur mit dem Einverständnis der Betroffenen zulässig ist (Abs. 1); das gleiche gilt für Daten, die nicht in automatisierten Verfahren, aber in Dateiform verarbeitet werden, denn die öffentliche Bekanntgabe derartiger Informationen ist im datenschutzrechtlichen Sinne für die regelmäßige Aufgabenerfüllung der speichernden Behörden nicht erforderlich und in der Abwägung mit dem Übermittlungsinteresse dürften die schutzwürdigen Belange der Betroffenen regelmäßig überwiegen (Absatz 2).

Eine Übermittlung von personenbeziehbaren Angaben an die Presse ist danach ohne Einwilligung der Betroffenen ebenfalls ausgeschlossen.

Dem besonderen Informationsanspruch des Parlaments ist durch § 92 a der Geschäftsordnung des Landtags Rechnung getragen. In Fällen, in denen Datenschutz oder sonstige Geheimhaltungsgründe der Beantwortung einer Kleinen Anfrage entgegenstehen, ist die Antwort im zuständigen Ausschuß in nichtöffentlicher oder vertraulicher Sitzung zu erteilen; der Fragesteller ist berechtigt, an der Sitzung des Ausschusses teilzunehmen.

8.4.3 Einzelübermittlung personenbeziehbarer Daten

Im Grundsatz greifen diese Überlegungen auch dann Platz, wenn es nicht um die Veröffentlichung der Daten, also die Übermittlung an einen unbestimmten Empfängerkreis, sondern um die Auskunftserteilung in Einzelfällen an Dritte geht.

Hier ist freilich zu differenzieren, denn nur für die Übermittlung an private Personen oder Stellen gilt § 7 LDatG. Für die Übermittlung an Stellen innerhalb des öffentlichen Bereichs – also an Behörden und sonstige öffentliche Stellen – ist § 6 LDatG heranzuziehen. Die Übermittlung wäre nach dieser Vorschrift zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.

Diese Vorschrift kann nach Auffassung der DSK zur Zeit noch als Übermittlungsgrundlage herangezogen werden, auch wenn vor dem Hintergrund des Volkszählungsurteils des Bundesverfassungsgerichts für die Zukunft normenklare bereichsspezifische Übermittlungregelungen zu fordern sind. Bei der Anwendung des Erforderlichkeitsbegriffs ist jedoch ein strenger Maßstab anzulegen, der dem Eingriffscharakter der Datenübermittlung Rechnung trägt.

Im übrigen kann eine Datenübermittlung auf der Grundlage des § 6 des LDatG allenfalls in solchen Fällen in Betracht kommen, in denen davon auszugehen ist, daß die in einem Kataster gespeicherten Daten richtig sind. Angaben zu altlastverdächtigen Flächen sind nach § 13 Abs. 2 LDatG zu sperren, da sich – solange der Verdacht nicht bestätigt oder ausgeräumt wurde – weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen läßt. Auf das Bestreiten der Richtigkeit von Daten durch den Betroffenen kommt es dabei nicht an, denn nach § 13 Abs. 4 LDatG ist die Sperrung beim Vorliegen der Voraussetzungen auch von Amts wegen vorzunehmen. Die gesperrten Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt oder sonstwie genutzt werden, es sei denn, daß die Nutzung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene der Nutzung zugestimmt hat.

8.4.4 Auskunftserteilung an Betroffene

Nach § 12 LDatG haben Betroffene grundsätzlich einen Auskunftsanspruch, der sich auch auf gesperrte Daten bezieht. Eine Verpflichtung, Betroffene über die erstmalige Speicherung von Daten zu benachrichtigen, ist dem Landesdatenschutzgesetz nicht zu entnehmen.

8.4.5 Offenbarung von Daten, auf die das Landesdatenschutzgesetz nicht anzuwenden ist

Die Vorschriften des Landesdatenschutzgesetzes finden keine Anwendung auf Daten, die sich auf juristische Personen des öffentlichen oder privaten Rechts beziehen. Dies bedeutet freilich nicht, daß diese Daten völlig ungeschützt sind. Sie unterliegen vielmehr dem Geheimhaltungsgrundsatz, der das Verwaltungsverfahren bestimmt (§ 30 Verwaltungsverfahrensgesetz), als Ausdruck eines allgemeinen Rechtsgedankens aber auch außerhalb des Verwaltungsverfahrens anzuwenden ist (vgl. Tz. 20.1). Nach der erwähnten Bestimmung haben die Beteiligten Anspruch darauf, daß ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden. Befugt ist eine Offenbarung dann, wenn der Betroffene zustimmt. Eine Offenbarung an andere öffentliche Stellen ist nach Normzweck und Interessenlage in Analogie zu § 6 LDatG ebenfalls zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist.

8.4.6 Zusammenfassung

Nach geltendem Datenschutzrecht ist die Übermittlung – Offenbarung – von Daten, die in Abfalldeponiekatastern oder Altlastenkatastern gespeichert sind, ohne Zustimmung der betroffenen Grundstückseigentümer nur dann zulässig, wenn es sich um verifizierte Erhebungsergebnisse handelt und Übermittlungsempfänger eine Behörde oder sonstige öffentliche Stelle ist. In allen anderen Fällen besteht ein Zustimmungsvorbehalt.

Ob die Gesetzeslage und die daraus zu ziehenden Folgerungen den Bedürfnissen der Praxis entspricht, kann nach derzeitigem Erkenntnisstand von der DSK nicht beurteilt werden. Grundsätzlich ist zu begrüßen, daß bei der Diskussion abfallrechtlicher Probleme auch Datenschutzfragen behandelt werden. Die DSK wird darauf hinwirken, daß bei der Novellierung des Abfallgesetzes angemessene bereichsspezifische Datenerhebungs- und Übermittlungsregelungen geschaffen werden.

8.5 Atomrechtliches Genehmigungsverfahren Kernkraftwerk Mülheim-Kärlich

8.5.1 Vorbereitung des Erörterungstermins

Das zum Zeitpunkt der Berichtsvorlage noch nicht abgeschlossene Genehmigungsverfahren für das Kernkraftwerk Mülheim-Kärlich findet in der Öffentlichkeit große Beachtung. Ein bedeutendes Thema ist dabei die Anwendung automatisierter Datenverarbeitungsverfahren für die Vorbereitung und Durchführung des Erörterungstermins und die Bekanntgabe der Einwendungen an die Antragsteller – RWE und ein aus mehreren Unternehmen bestehendes Konsortium –.

Das für die Durchführung des Genehmigungsverfahrens zuständige MUG rechnete mit 100 000 bis 200 000 Einwendungen im Genehmigungsverfahren – vorwiegend Einzeleinwendungen – und mit einer dementsprechend hohen Zahl von Teilnehmern an dem nach der Atomrechtlichen Verfahrensordnung nichtöffentlichen Erörterungstermin. Es ging davon aus, daß der Erörterungstermin – Einlaßkontrolle und Sitzungsleitung – mit einem vertretbaren Zeit-, Sach- und Personalaufwand nicht ohne Zuhilfenahme der automatisierten Datenverarbeitung durchzuführen sei.

Die Tatsache, daß sich die ursprünglichen Annahmen bezüglich der Einwenderzahl als Fehleinschätzungen erwiesen – es wurden nur rund 66 000 Einwendungen erhoben, davon 191 Einzeleinwendungen und 22 Sammeleinwendungen unterschiedlichen Inhalts – führte nicht zu einer Änderung der Datenverarbeitungskonzeption.

Die Einwendungen wurden „gescannt" (maschinelles Klarschriftlesen) und in der Originalfassung auf einem maschinenlesbaren Datenträger abgebildet. Den Zugriff auf die Dokumente vermittelt eine gesonderte Datei, in der die Einwenderadressen gespeichert sind.
Da die für die Datenerfassung und -verarbeitung erforderlichen personellen und maschinellen Kapazitäten im Ministerium nicht zur Verfügung standen, wurde ein privates Serviceunternehmen beauftragt, die Geräte zur Verfügung zu stellen und die Arbeiten durchzuführen.

8.5.2 Bekanntgabe der Einwenderadressen an die Antragsteller

Im Mittelpunkt der datenschutzrechtlichen Beurteilung des Verfahrens stand zunächst die vom Ministerium beabsichtigte Weitergabe einer Kopie der Bildplatte mit den gespeicherten Einwendungen – einschl. rund 66 000 Einwenderadressen – an die Antragsteller. Rechtsgrundlage von Datenübermittlungen in diesem Zusammenhang kann nur § 7 Abs. 2 der Atomrechtlichen Verfahrensordnung sein, der die Genehmigungsbehörde verpflichtet, den „Inhalt" der Einwendungen dem Antragsteller bekanntzugeben. Durch den Wortlaut der Vorschrift, so die Meinung der Kommission, ist die Bekanntgabe der vollständigen Einwenderadresse an den Einwender nicht gedeckt. Ein Übermittlungsinteresse des Antragstellers bestehe lediglich bezüglich des sachlichen Vorbringens und des Wohnorts als Adreßbestandteil.

Sie ließ sich bei dieser Entscheidung von folgenden Erwägungen leiten:

Die Weitergabe der im Atomrechtlichen Genehmigungsverfahren erhobenen Einwendungen in personenbezogener Form ist als Eingriff in das Recht auf informationelle Selbstbestimmung – das Recht, selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen – zu qualifizieren. Dieser Eingriff bedarf einer normenklaren gesetzlichen Grundlage, die dem Grundsatz der Verhältnismäßigkeit entsprechen muß. Eine Weitergabe von Einwendungen in personenbezogener Form darf demzufolge nur dann erfolgen, wenn eine ausdrückliche verfassungsgemäße Rechtsgrundlage hierfür herangezogen werden kann. § 7 Abs. 2 Satz 2 der Atomrechtlichen Verfahrensordnung bietet bezüglich der Bekanntgabe der Einwenderadressen keine den verfassungsrechtlichen Anforderungen entsprechende Grundlage. Dies folgt schon daraus, daß die Auslegung der wortgleichen Bestimmung in § 12 der Neunten Bundesimmissionsschutzverordnung, die das Ministerium zur Begründung seiner Auffassung heranzog und als „entstehungsgeschichtliche Wurzel" der entsprechenden Regelung in der Atomrechtlichen Verfahrensordnung bezeichnete, in dem fraglichen Punkt durchaus umstritten ist. Der Niedersächsische Umweltminister teilte dem dortigen Datenschutzbeauftragten hierzu folgendes mit: „Danach teile ich Ihre Rechtsauffassung, daß Name und Anschrift von Einwendern nicht ‚Inhalt' der Einwendungen im Sinne des § 12 der Neunten Bundesimmissionsschutzverordnung sind, obgleich diese Ansicht umstritten ist." Die gleiche Auffassung vertrat der Niedersächsische Minister für Bundesangelegenheiten bereits im Jahre 1985. In einer Rundverfügung wurden die Bezirksregierungen gebeten, Namen und Adressen von Einwendern an die Antragsteller nur auf ausdrückliche, begründete Anforderung im Einzalfalle weiterzugeben. „Dazu muß der Antragsteller ein berechtigtes Interesse darlegen. Im übrigen dürfen durch die Weitergabe schutzwürdige Belange von Einwendern nicht beeinträchtigt werden."

Außerdem wurde festgestellt, daß in Hessen die personenbezogene Weitergabe von Einwendungen in atomrechtlichen Verfahren regelmäßig unterblieben ist; in Bayern – Wiederaufbereitungsanlage Wackersdorf – erfolgte sie nur in Einzelfällen, etwa nach den Auslegungsgrundsätzen, wie sie für das Immissionsschutzverfahren in Niedersachsen formuliert wurden.

Bei der Auslegung einer nicht normenklaren Rechtsvorschrift ist nach der Rechtsprechung des Bundesverfassungsgerichts derjenigen Interpretation der Vorzug zu geben, die den Grundrechten – hier dem Recht auf informationelle Selbstbestimmung – zu einer größtmöglichen Wirksamkeit verhilft. Im Mittelpunkt einer solchen Auslegung steht der Verfassungsgrundsatz der Verhältnismäßigkeit, der das Erforderlichkeitsprinzip umfaßt.

Soweit vom Ministerium zur Begründung der Erforderlichkeit der Datenübermittlung vorgetragen wurde, daß sich die mögliche Betroffenheit häufig erst aus der Anschrift ergebe, die auf die Lage eines Nachbargrundstücks zurückschließen lasse, so konnte diesem Gesichtspunkt durch Übermittlung des Wohnortes des Einwenders hinreichend Rechnung getragen werden.

Nach dem „Sasbach-Urteil" des Bundesverwaltungsgerichts vom 17. Juni 1980 (BVerwGE 6O, 297,311) muß die Einwendung erkennen lassen, welches seiner Rechtsgüter der Einwender als gefährdet ansieht. Er muß dieses Rechtsgut bezeichnen und die befürchtete Beeinträchtigung darlegen. Danach kommt es in aller Regel auf den sachlichen Vortrag des Einwenders an und nicht auf seinen Namen.

Zusammenfassend kam die DSK zu dem Ergebnis, daß die Übermittlung der genauen Adresse von Einwendern an die Antragsteller im Atomrechtlichen Genehmigungsverfahren nicht erforderlich ist. Eine verfassungskonforme Auslegung der nicht normenklaren Bestimmung des § 7 Abs. 2 Satz 1 der Atomrechtlichen Verfahrensordnung kann daher nur zu dem Ergebnis führen, daß die Übermittlung im Grundsatz unzulässig ist. Ausnahmen können allenfalls dann gerechtfertigt sein, wenn im Einzelfall ein berechtigtes Interesse durch den Antragsteller dargelegt wird und durch die Weitergabe schutzwürdige Belange von Einwendern nicht beeinträchtigt werden.

Das Ministerium hat sich dieser Rechtsauffassung nicht angeschlossen, sich dessen ungeachtet aber bereit erklärt, der Empfehlung der DSK nachzukommen. Dementsprechend wurde die Öffentlichkeit darüber informiert, daß keine personenbezogenen Daten der Einwender an die Antragsteller weitergeleitet werden. Die Bekanntgabe des Inhalts der Einwendungen sollte vielmehr in der Weise erfolgen, daß der Einwendungstext kopiert, die Adressen hierbei aber abgedeckt werden.

Die Verarbeitung der Einwenderdaten im Auftrag des Ministeriums durch ein Serviceunternehmen außerhalb des öffentlichen Bereichs sah die DSK grundsätzlich als zulässig an. Sie forderte jedoch, daß dem Unternehmen detaillierte Weisungen für die Datenverarbeitung erteilt werden und vertraglich sichergestellt wird, daß die Vorschriften des Landesdatenschutzgesetzes vom Auftragnehmer beachtet werden. Sie hielt es weiter für erforderlich, ein Prüfungsrecht für den Auftraggeber und die DSK einräumen zu lassen und ein Recht auf fristlose Kündigung bei einer Verletzung von Datenschutzbestimmungen zum Vertragsgegenstand zu machen.

Die von der DSK zur Frage der Erforderlichkeit der Adreßübermittelung vertretene Auffassung wurde vom RWE mittelbar durch die Erklärung bestätigt, daß die Adressen nicht benötigt würden.

8.5.3 Ergebnisse örtlicher Prüfungen

Auf Beschluß der DSK wurde der Einsatz der automatisierten Datenverarbeitung für die Vorbereitung und Durchführung des atomrechtlichen Erörterungstermins für das Kernkraftwerk Mülheim-Kärlich in datenschutzrechtlicher Hinsicht überprüft. Kontrollmaßnahmen wurden sowohl am Sitze des beauftragten Unternehmens wie auch während des Erörterungsverfahrens in Mülheim-Kärlich durchgeführt. Bei beiden Prüfungen wurden keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt. Die Datenverarbeitung war in dem praktizierten Umfange zulässig, die Datensicherheit entsprach dem Stand der Technik und wurde von dem beauftragten Unternehmen beachtet. Im einzelnen ergab die Prüfung, daß keinerlei Abgleich der erfaßten Daten von Einwendern mit anderen Datenbeständen im öffentlichen oder nichtöffentlichen Bereich stattfand, daß keine Zugriffsmöglichkeit auf andere Datenbestände existierte und daß im automatisierten Verfahren keine Daten an die Antragsteller – etwa durch Weitergabe einer Kopie der Bildplatte, wie ursprünglich vorgesehen – übermittelt wurden. Die Öffentlichkeit wurde über diese Prüfungsergebnisse, wie auch über die vorangegangene Auseinandersetzung mit dem Ministerium zur Frage der rechtlichen Zulässigkeit der Datenübermittlung unterrichtet.

8.5.4 Versehentliche Datenübermittlung durch das Ministerium an das RWE

Aufgrund der öffentlichen Erklärung eines Vorstandssprechers des RWE wurde bekannt, daß, entgegen der Zusage des Ministeriums, doch in einer zunächst nicht genau bekannten Zahl von Fällen Einwendungen mit den Einwenderadressen als Kopie an das Unternehmen weitergegeben wurden. Der zuständige Staatssekretär des Ministeriums, in einer Kommissionssitzung zum Sachverhalt befragt, erklärte, daß beim Kopieren der Einwendungen versehentlich nicht alle Adressen abgedeckt wurden. Es seien insgesamt etwa 300 Einwenderadressen an das RWE übermittelt, dort aber, noch bevor die Einwendungen in den Geschäftsgang gelangten, gelöscht worden.

Die DSK stellte förmlich fest, daß, die Richtigkeit der von ihr in der Frage der Adreßweitergabe vertretenen Rechtsauffassung vorausgesetzt, mit der Datenübermittlung gegen geltendes Recht verstoßen wurde, daß das MUG aber zumindest gegen die der DSK und der Öffentlichkeit gegebene Zusage verstoßen habe, keine Adreßdaten zu übermitteln. Sie gab ihrem Befremden darüber Ausdruck, daß ihren Beauftragten bei den örtlichen Feststellungen in Mülheim-Kärlich eine unzutreffende Sachverhaltsdarstellung gegeben wurde.

8.5.5 Reaktionen der Öffentlichkeit

Die DSK fand mit ihrem Eintreten für die Persönlichkeitsrechte der Einwender ein starkes und positives Echo in der Öffentlichkeit. In einer Reihe von Fällen wandten sich Betroffene an die Kommission und erbaten Auskünfte oder die Überprüfung von Übermittlungsvorgängen.

Aufgrund der Berichterstattung in den Medien fand ein Vorgang starke Beachtung, der die Datenverarbeitung im Zusammenhang mit der Einlaßkontrolle bei dem Erörterungstermin betraf. Ein Einwender behauptete, die Adreßdaten seiner geschiedenen Frau seien zusammen mit seinen Adreßdaten beim Abruf auf dem Bildschirm dargestellt worden. Er sah dies als Beweis dafür an, daß bei der Einlaßkontrolle auf Daten aus anderen öffentlichen Registern zugegriffen werden könne.

Die Überprüfung ergab, daß bei der Bildschirmrecherche jeweils eine Vielzahl von Einwenderadressen in alphabetischer Reihenfolge sichtbar werden. Es war also im Grundsatz nicht auszuschließen, daß, wie behauptet, auch die Adreßdaten der geschiedenen Frau mit gleichem Namen erkennbar waren. Voraussetzung hierfür war jedoch, daß auch sie eine Einwendung erhoben hatte. In der Tat fand sich eine namensgleiche Einwenderin mit gleichem Wohnort, von der angenommen wurde, daß es sich um die geschiedene Ehefrau handele.

Die Richtigkeit dieser Recherchen wurde in der Öffentlichkeit bestritten mit der Behauptung, die geschiedene Frau habe einen anderen Namen, wohne an einem anderen Ort und habe nach ihrem eigenen Bekunden keine Einwendung in dem Genehmigungsverfahren erhoben. Die daraufhin von der DSK an den Beschwerdeführer gerichtete Aufforderung, zum Zwecke einer nochmaligen Überprüfung den Namen und die Anschrift der geschiedenen Frau mitzuteilen, blieb unbeantwortet.

Die DSK wertet den Vorgang abschließend als den Versuch des Einwenders, durch Verhinderung der Sachverhaltsaufklärung eine von vornherein falsche Behauptung möglichst lange medienwirksam aufrecht zu erhalten. Sie stellt diesen Vorgang deshalb so ausführlich dar, weil er im Landtag zum Gegenstand einer Kleinen Anfrage gemacht wurde.

8.5.6 Fazit

Die verhältnismäßig breite Darstellung der datenschutzrelevanten Vorgänge um das Genehmigungsverfahren für das Kernkraftwerk Mülheim-Kärlich erscheint der DSK geboten, weil das Verfahren noch nicht abgeschlossen ist und die Öffentlichkeit bisher nicht umfassend unterrichtet wurde. Die DSK hat sich bei der Bewertung der Vorgänge streng an datenschutzrechtlichen Gesichtspunkten orientiert. Eine Beurteilung der Vorbereitung und der Durchführung des Anhörverfahrens unter anderen Aspekten liegt außerhalb ihrer Zuständigkeit. Dennoch bleibt folgendes festzuhalten: Der Einsatz der automatisierten Datenverarbeitung ermöglicht die Aufgabenwahrnehmung in einer Weise, die bei einer Beschränkung auf herkömmliche Informationsmittel nicht vorstellbar ist. Da dem Verhandlungsleiter beispielsweise der Inhalt einer schriftlich vorgebrachten Einwendung in Sekundenschnelle zur Verfügung steht, ist es ihm möglich, den jeweiligen Sachvortrag im Erörterungstermin in einer von der Verfahrensordnung zwar zugelassenen, sonst aber kaum praktikablen Weise auf die Erläuterung des schriftlich Vorgebrachten einzuschränken. Daß ferner das Vorhandensein der Vielzahl technischer Geräte und die für die Betroffenen undurchschaubaren Verarbeitungsprozeduren zu Vorbehalten hinsichtlich der Ordnungsmäßigkeit des Verfahrens führen können, ist wohl jedem einsichtig, der den Technikeinsatz vor Ort erlebte. Daß schließlich das Beharren auf Rechtsstandpunkten ohne Rücksicht auf die wirkliche Bedeutung der Sache und die praktischen Notwendigkeiten zu Mißtrauen in der Bevölkerung und Verärgerung führt, darf nicht verwundern. Den für die Durchführung des Genehmigungsverfahrens Verantwortlichen ist anzuraten, Datenschutzprobleme künftig mit mehr Sensibilität zu behandeln.

8.6 Sicherheitsüberprüfung von Fremdpersonal, das im Kernkraftwerk Mülheim-Kärlich beschäftigt ist

Aufgrund einer Anmeldung des MUG hatte sich die DSK mit der Frage zu befassen, ob es zulässig ist, daß personenbezogene Daten von sogenanntem Fremdpersonal, das im Kernkraftwerk Mülheim-Kärlich zu Arbeitszwecken eingesetzt werden soll, zur Durchführung einer Sicherheitsüberprüfung in einem PC gespeichert werden dürfen. Problematisch ist in diesem Zusammenhang, daß den Personen, die sich mit einer Sicherheitsüberprüfung nicht einverstanden erklären und damit keine Auskünfte über eigene personenbezogene Daten erteilen, dadurch ein Nachteil entstehen kann, daß sie ihren Arbeitsplatz mangels Einsatzmöglichkeit verlieren. Nach § 5 Abs. 2 S. 2 LDatG darf einer Person dann, wenn keine Rechtsvorschrift zur Auskunftserteilung besteht, wegen einer Verweigerung der Auskunft kein Nachteil entstehen.

Aus den §§ 4, 6, 7, 9 und 9 b AtomG läßt sich für Fremdpersonal, das in einem Kernkraftwerk eingesetzt werden soll, eine Auskunftspflicht über personenbezogene Daten nicht entnehmen. Trotzdem wurde von der DSK die Notwendigkeit anerkannt, daß auch Fremdpersonal, das in einem Kernkraftwerk eingesetzt wird, einer Sicherheitsüberprüfung zu unterziehen ist, da ansonsten erhebliche Sicherheitsinteressen tangiert würden. Bedenken gegen die in Rheinland-Pfalz durchgeführte Praxis wurden daher von der DSK nicht erhoben. Sie hat jedoch empfohlen, daß über den Bundesrat eine Ergänzung der atomrechtlichen Vorschriften angestrebt werden sollte, aus der sich ergeben müßte, daß sich auch Fremdpersonal, das zur Arbeit in einem Kernkraftwerk zugelassen werden will, einer Sicherheitsüberprüfung zu unterziehen und die dazu erforderlichen Auskünfte zu erteilen hat.

Ebenfalls wurde angeregt, daß die zu überprüfenden Personen schriftlich darauf hingewiesen werden, daß sie sich, soweit eine Entscheidung für sie negativ ausfallen sollte, an den Datenschutzbeauftragten mit der Bitte um datenschutzrechtliche Überprüfung wenden können. Auf die Erklärungsbögen sollte schließlich noch ein Hinweis auf die im Zusammenhang mit der Sicherheitsüberprüfung erfolgten Speicherungen eingetragen werden.

Mit Schreiben vom 31. Januar 1989 teilte das MUG mit, daß das Land Rheinland-Pfalz wegen der Frage der Ergänzung der atomrechtlichen Vorschriften den zuständigen Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit gebeten habe, eine Klärung herbeizuführen. Das MUG teilte der DSK weiterhin mit, daß die Betroffenen darüber informiert werden, daß sie

sich bei einer negativen Entscheidung an die DSK wenden können und daß personenbezogene Daten über sie automatisiert gespeichert werden. Mittlerweile wurde vom Bundestag § 12 b (Überprüfung der Zuverlässigkeit zum Schutz gegen Entwendung oder erheblicher Freisetzung radioaktiver Stoffe) in das AtomG eingeführt. Diese Vorschrift ist am 1. November 1989 in Kraft getreten.

9 Gesundheitswesen

9.1 Gesundheitsdienstgesetz

Die Arbeit der Gesundheitsämter in Rheinland-Pfalz stützt sich noch immer im wesentlichen auf das „Gesetz über die Vereinheitlichung des Gesundheitswesens" vom 3. Juli 1934 und die hierzu ergangenen Durchführungsverordnungen aus dem Jahre 1935. Die genannten Rechtsgrundlagen entsprechen kaum noch den heutigen Anforderungen an eine moderne öffentliche Gesundheitspflege. Es fehlt darüber hinaus an normenklaren Befugnissen zur Erhebung und Verarbeitung von personenbezogenen Daten, wie sie von der Konferenz der Datenschutzbeauftragten und der DSK in der Entschließung vom 8. März 1984 zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts gefordert wurden (vgl. 10. Tätigkeitsbericht, Anlage 1, S. 59).

Die Erfahrungen aus der Wahrnehmung von Kontrollaufgaben im Bereich der Gesundheitsverwaltung, aus der Bearbeitung von Eingaben und aus der Teilnahme von Vertretern der DSK an Dienstbesprechungen oder Veranstaltungen, die dem Erfahrungsaustausch zwischen Mitarbeitern der Gesundheitsverwaltung dienten, unterstreichen die Forderung nach einer gesetzlichen Neuordnung dieses Bereichs. Wesentliche Grundfragen zur rechtlichen Stellung der Ärzte in der Gesundheitsverwaltung, des ärztlichen Hilfspersonals und der in den sozialpsychiatrischen Diensten tätigen Mitarbeiter (Sozialarbeiter) sind ungeklärt.

Initiativen sind um so dringlicher, als die Gesundsheitsverwaltung in Rheinland-Pfalz an der Schwelle steht zum Einsatz autonomer automatisierter Verfahren für die Aufgabenerfüllung. Im Blick auf die außerordentlich hohe Sensitivität der Informationsverarbeitung im Gesundheitsbereich kann ein Rechnereinsatz grundsätzlich nur dann akzeptiert werden, wenn die Aufgaben und Befugnisse der Gesundheitsverwaltung gegenüber den Bürgern und ihre Zusammenarbeit mit anderen Stellen normenklar geregelt sind und die Einhaltung dieser Regelungen durch organisatorische Vorkehrungen gesichert ist.

Der Minister für Umwelt und Gesundheit stimmt dieser Beurteilung im Grundsatz zu. Er teilte der DSK mit, daß in Rheinland-Pfalz schon lange an einem entsprechenden Gesetzentwurf gearbeitet werde. Der aktuelle Entwurf, der wegen der Überlegungen bezüglich einer Funktionalreform, insbesondere wegen der Frage, ob die Behörden des öffentlichen Gesundheitsdienstes weiterhin selbständig bleiben sollen, noch nicht die Kabinettsreife erlangt hat, sehe statistikrechtliche und datenschutzrechtliche Normen vor, die sich an den Maßstäben orientierten, die das Bundesverfassungsgericht im Volkszählungsurteil gesetzt habe. Er sicherte zu, daß die DSK zu dem Entwurf angehört werde.

9.2 Datenschutzrechtliche Grundsatzfragen, die einer gesetzgeberischen Lösung bedürfen

9.2.1 Verwertung von Informationen

Ein Großteil der vom öffentlichen Gesundheitsdienst wahrzunehmenden Aufgaben ist hoheitlicher Natur. Im Vordergrund stehen dabei die gesundheitspolizeilichen Aufgaben, etwa bei der Ausführung des Bundesseuchengesetzes oder des Geschlechtskrankheitengesetzes. Daneben werden die Gesundheitsämter im Rahmen ihrer dienstlichen Aufgaben vielfach auch beratend und aufklärend tätig (beispielsweise Familienberatung, Schwangerenberatung, gesundheitliche Beratung bei Suchtkranken). Der Bürger kann diese Beratungs-, Aufklärungs- und Dienstleistungsangebote des öffenlichen Gesundheitsdienstes annehmen; er kann zur Annahme dieser Angebote aber nicht verpflichtet werden.

In beiden Funktionsbereichen unterliegen Ärzte und ärztliches Hilfspersonal Geheimhaltungspflichten, die nach § 203 StGB strafbewehrt sind. Dabei ist strafrechtlich geschützt nicht nur das Individualinteresse an der Geheimhaltung bestimmter Tatsachen; vorrangig ist vielmehr der sozialpolitische Aspekt, nämlich das allgemeine Vertrauen in die Verschwiegenheit der Angehörigen bestimmter Berufe.

Diese der strafrechtlichen Bestimmung zugrunde liegenden Zielsetzungen werden – in jeweils unterschiedlicher Intensität – berührt, wenn Informationen aus der freiwilligen Inanpruchnahme gesundheitsdienstlicher Leistungen zur Aufgabenwahrnehmung in anderen Bereichen – insbesondere Eingriffsverwaltung – verwendet werden.

Auch die Inanspruchnahme von Informationen aus der gesundheitspolizeilichen Tätigkeit für Beratungs-, Aufklärungs- und Dienstleistungszwecke ist nicht völlig unproblematisch; in aller Regel wird hier indessen vom Vorliegen der Einwilligung des Betroffenen auszugehen sein.

Das dargestellte Problem bedarf dringend einer gesetzgeberischen Lösung. Zu bezweifeln ist, ob ein Verwertungsverbot, wie es Artikel 6 des Bayerischen Gesundheitsdienstgesetzes zu entnehmen ist, ausreicht. Im Grundsatz ist die Forderung nach weitergehenden Offenbarungsbeschränkungen und Abschottungsbestimmungen zu erheben.

9.2.2 Sozialpsychiatrischer Dienst

Die bei den Sozialpsychiatrischen Diensten der Gesundheitsämter tätigen staatlich anerkannten Sozialarbeiter sind Angehörige einer in § 203 Abs. 1 StGB genannten Berufsgruppe, d. h. die Verletzung von Verschwiegenheitspflichten durch einen Sozialarbeiter ist nach dieser Vorschrift strafbar.

Ebenso wie Ärzte des Gesundheitsamtes sind sie bei der Wahrnehmung ihrer Aufgaben indessen in das hierarchische System der Behörde eingebunden, d. h., die jeweiligen Vorgesetzten sind weisungs- und kontrollbefugt. In Wahrnehmung dieser Weisungs- und Kontrollaufgaben wird in aller Regel der Anspruch auf vollständige Information über die Tätigkeit der Sozialarbeiter, insbesondere auch über den Inhalt von Beratungsgesprächen mit Klienten, erhoben.

Vertreter der DSK wurden schon wiederholt auf die Offenbarungsproblematik vor dem Hintergrund des § 203 StGB angesprochen. Diese Problematik stellt sich ganz besonders deutlich in solchen Fällen, in denen weder eine ausdrückliche Einwilligung des Geheimnisträgers in die Offenbarung vorliegt, noch von einer konkludenten oder mutmaßlichen Einwilligung ausgegangen werden kann. Nicht selten, so wurde von Sozialarbeitern bei Gesundheitsämtern erklärt, beharrten die Klienten sogar ausdrücklich darauf, daß die bei der Wahrnehmung von Beratungsaufgaben anvertrauten Informationen nicht – auch nicht an Vorgesetzte oder gar Kollegen – weitergegeben werden.

Von den Aufsichtsbehörden wurde hierzu die Auffassung vertreten, daß Sozialarbeiter befugt und sogar verpflichtet seien, dem dienstvorgesetzten Arzt fremde Geheimnisse weiterzugeben, wenn dies der Aufgabenerfüllung des Gesundheitsamtes diene.

Demgegenüber ist das Ministerium der Ansicht, daß nicht alle personenbezogenen Daten, die der Aufgabenerfüllung des Gesundheitsamtes „dienen", sondern nur solche, die zur Aufgabenerfüllung des Gesundheitsamtes erforderlich sind und die von einem Sozialarbeiter in unmittelbarem Zusammenhang hiermit erhoben worden sind, der dienstlichen Informationspflicht unterfallen. Die Informationspflicht bestehe nicht bei solchen Daten, die nur „bei Gelegenheit" der Erfüllung von Dienstaufgaben in Erfahrung gebracht wurden. Ohne das ausdrückliche Einverständnis des Probanden dürfe der Sozialarbeiter die zuletzt genannten personenbezogenen Daten nicht offenbaren.

Dieser Lösungsansatz ist ebenfalls nicht unproblematisch. Die Anbindung von Offenbarungsbefugnissen an die „Aufgabenerfüllung des Gesundheitsamtes" kann jedenfalls nicht wesentlich weiterführen, so lange diese Aufgaben nicht mit größtmöglicher Genauigkeit gesetzlich beschrieben und den Funktionseinheiten des Gesundheitsamtes zugewiesen sind. Es ist zwar zu begrüßen, daß das Ministerium den in der Vergangenheit von den leitenden Ärzten der Gesundheitsämter erhobenen umfassenden Informationsanspruch nicht mehr anerkennt, dennoch besteht weiterer Regelungsbedarf, der wohl nur vom Gesetzgeber zu befriedigen ist.

9.3 Auskunftserteilung durch Gesundheitsämter

Die Dringlichkeit einer gesetzlichen Neuordnung des Gesundheitsdienstes wird auch dadurch unterstrichen, daß bezüglich der Pflicht zur Auskunftserteilung erhebliche Rechtsunsicherheit besteht. Die Folge dieser Rechtsunsicherheit ist in aller Regel eine Einschränkung der Informationsmöglichkeiten des Betroffenen. Dieser hat keine Möglichkeit, die Begründetheit einer Entscheidung nachzuvollziehen.

Die Schilderung eines konkreten Falles soll dies verdeutlichen:

In einer Eingabe wurde der DSK mitgeteilt, daß in einem Gesundheitsamt ein Bewerber um einen Ausbildungsplatz als Bankkaufmann auf Ersuchen einer Stadtsparkasse amtsärztlich untersucht wurde. Es wurde in der Eingabe gerügt, daß der zuständige Arzt nicht bereit war, dem Untersuchten eine Kopie des gesundheitsärztlichen Zeugnisses zu überlassen. In einem Schreiben an den Betroffenen wurde dies wie folgt begründet: „Grundlage dafür, daß eine Kopie des amtsärztlichen Zeugnisses nicht vom Gesundheitsamt an den Untersuchten geschickt werden darf, ist die Tatsache, daß diese amtsärztliche Untersuchung aufgrund eines Amtshilfeersuchens einer Behörde erfolgte, nicht vom zu Untersuchenden beantragt ist (und auch von Privatpersonen nicht beantragt werden kann). Unsere Bestimmungen untersagen uns ausdrücklich die Weitergabe bzw. Mitteilung des Untersuchungsergebnisses an andere Stellen als die anfordernde Dienststelle."

Das MUG als oberste Aufsichtsbehörde vertrat zunächst folgende Auffassung: „Das amtsätztliche Gutachten, das im Auftrag eines Dritten erfolgt, darf dem Untersuchten nicht in Abschrift oder zur Einsichtnahme überlassen werden. Allein der Auftraggeber ist Herr des Verfahrens."

Obwohl die DSK zuvor die Stellungnahme des Gesundheitsamtes als unzutreffend bezeichnet hatte, machte das Ministerium dieses Ergebnis seiner Beurteilung ohne jede Abstimmung mit der DSK durch ein Rundschreiben an alle Gesundheitsämter bekannt.

Die DSK trat dieser Rechtsauffassung und Sachbehandlung entgegen. Sie wies darauf hin, daß es in der freien Entscheidung des Betroffenen liegt, der Aufforderung zur Teilnahme an einer Einstellungsuntersuchung nachzukommen. Ebenso ist es seiner freien Entscheidung überlassen, ob und ggf. welchen Stellen Untersuchungsergebnisse offenbart werden. Da gesetzliche Eingriffsbefugnisse nicht existieren, hat der Betroffene selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Das Bundesverfassungsgericht hat aus dem Recht auf informationelle Selbstbestimmung unmittelbar eine Pflicht zur Aufklärung abgeleitet. Demnach ist sicherzustellen, daß der Betroffene sich zuverlässig darüber unterrichten kann, wer was wann bei welcher Gelegenheit über ihn weiß. Zwar ist auch dieses Auskunftsrecht im überwiegenden Allgemeininteresse einschränkbar; für Einstellungsuntersuchungen der Gesundheitsämter ist dies aber nicht geschehen und es ist, anders als beispielsweise im Sicherheitsbereich, auch kein Grund für eine Auskunftsbeschränkung erkennbar.

Ergänzend war darauf hinzuweisen, daß der Betroffene, wenn die Anwendungsvoraussetzungen des Landesdatenschutzgesetzes vorlägen (Datenverarbeitung in automatisierten Verfahren, Dateiverarbeitung), nach § 12 dieses Gesetzes ein Recht auf Auskunft über die gespeicherten Daten hätte. Nach Absatz 2 dieser Vorschrift könnte dieses Recht nur eingeschränkt werden, wenn dies zum Schutze der Gesundheit des Betroffenen geboten ist.

Außerhalb des formalen Anwendungsbereichs des Landesdatenschutzgesetzes hat ein Beteiligter nach § 29 des Verwaltungsverfahrensgesetzes ein Akteneinsichtsrecht, wenn die Kenntnis des Akteninhalts zur Geltendmachung oder Verteidigung rechtlicher Interessen erforderlich ist. Eine ähnliche Regelung, ergänzt um Sonderbestimmungen für Angaben über gesundheitliche Verhältnisse, ist § 25 SGB X zu entnehmen. Soweit nach dieser Vorschrift Akteneinsicht zu gestatten ist, können die Beteiligten auch Auszüge oder Abschriften selbst fertigen oder sich Ablichtungen durch die Behörde erteilen lassen.

Das Landeskrankenhausgesetz schließlich statuiert in § 36 Abs. 5 für Patienten weitgehende Auskunfts- und Einsichtsrechte.

Das Volkszählungsurteil des Bundesverfassungsgerichts und die dargestellten Regelungsbeispiele kennzeichnen eine Rechtsentwicklung, die, auch wenn eine Neuordnung der gesundheitsärztlichen Tätigkeit durch den Landesgesetzgeber noch aussteht, zu beachten ist. Aufgrund der Rechtsprechung des Bundesverfassungsgerichts hat der Amtsarzt von einem grundsätzlich bestehenden Auskunftsanspruch auszugehen. Bestehende Regelungsdefizite können für eine Übergangszeit durch die analoge Anwendung anderer gesetzlicher Vorschriften (beisp. Begrenzung von Auskunftsansprüchen nach § 36 Abs. 5 LKG) ausgefüllt werden.

Das Ministerium hat schließlich diese Rechtsauffassung anerkannt und die nachgeordneten Behörden entsprechend unterrichtet. Es wies ergänzend darauf hin, daß „die mit der Nichtweitergabe der Untersuchungsergebnisse in Folge des Veto des Berechtigten möglicherweise einhergehenden negativen Folgen (z. B. Ablehnung der Einstellung durch den Arbeitgeber in spe) durch den Inhaber des Rechts auf informationelle Selbstbestimmung allein zu verantworten sind".

Die von der DSK unter Hinweis auf die Rechtsprechung des Bundesverfassungsgerichts (Entscheidung vom 15. Juni 1983, BVerfGE 64/229) ferner angesprochene Frage (die allerdings nicht vorrangig unter datenschutzrechtlichen Gesichtspunkten von Bedeutung ist), ob eine Amtshilfeverpflichtung der Gesundheitsämter gegenüber den Sparkassen besteht oder ob die kostenlose Durchführung von Einstellungsuntersuchungen nicht eine unzulässige Bevorzugung öffentlich rechtlich organisierter Sparkassen gegenüber privaten Banken darstellt, wurde vom MUG noch nicht abschließend beantwortet.

9.4 Schulgesundheitspflege

Die Verarbeitung personenbezogener Daten in automatisierten Verfahren steht nach § 9 LDatG unter dem Vorbehalt angemessener Datensicherungsmaßnahmen. Je empfindlicher die im automatisierten Verfahren zu verarbeitenden Daten sind, um so höher muß der Datensicherungsaufwand sein.

Bis vor wenigen Jahren noch waren Datensicherungsprobleme beim Einsatz von Personalcomputern nur in einem begrenzten Umfange lösbar. Die DSK hatte deshalb wiederholt Veranlassung darauf hinzuweisen, daß das Fehlen hardwaremäßiger und in das Betriebssystem implementierter Vorkehrungen die Verarbeitung besonders sensitiver Datenarten nicht zuläßt. Zu diesen Datenarten gehörten selbstverständlich personenbezogene medizinische Daten.

Seit einiger Zeit ist freilich eine Entwicklung zu beobachten, die den Forderungen nach technischer Unterstützung von Datensicherungsmaßnahmen entgegenkommt (vgl. Tz. 19). Damit werden, weil die Datensicherungsprobleme lösbar geworden sind, dem PC-Einsatz neue Anwendungsbereiche erschlossen.

Zu diesen Anwendungsbereichen gehört auch die Gesundheitsverwaltung, die im November 1988 für den Jugendärztlichen Dienst eine PC-gestützte Anwendung zum Datenschutzregister anmeldete. Das Verfahren bezweckt eine Verbesserung der Auswertung von Untersuchungsergebnissen und die schnellere Gewinnung detaillierter Erkenntnisse über Gesundheitsgefährdungen bei Kindern und Jugendlichen. Die mit dem PC-Einsatz einhergehende Rationalisierung der Verwaltungsarbeit soll zu einer Intensivierung der jugendärztlichen Arbeit führen.

Die Anmeldung zum Datenschutzregister betraf eine Pilotanwendung beim Gesundheitsamt Bingen. In der Endstufe der Verfahrensentwicklung sollen rund 120 in Rheinland-Pfalz tätige Schulärzte mit einem transportablen PC, einem sog. Laptop, ausgestattet werden, der zunächst dazu dient, die bei der Untersuchung erhobenen Daten unter Vermeidung von Papieraufzeichnungen zu erfassen und in personenbezogener Form zu speichern. In den Gesundheitsämtern sollen leistungsfähige PC eingesetzt werden, in die die Datenbestände aus dem Laptop ohne Namensangabe übernommen werden. Die Personenbeziehbarkeit der übernommenen Daten bleibt jedoch bestehen, da jeder Datensatz mit einer Nummer versehen ist, die ein Zusammenführen mit den im Laptop verbleibenden Referenzdaten ermöglicht.

Der Schularzt wird also, vereinfacht ausgedrückt, die bei der Untersuchung erhobenen Daten zum Zwecke der zentralen Auswertung in einer anonymisierten Form zur zentralen Verarbeitung an das Gesundheitsamt übergeben. Für die Wahrnehmung seiner jugendärztlichen Aufgaben kann er sie jederzeit zurückerhalten und, weil ihm die Referenzliste zur Verfügung steht, deanonymisieren.

Die Befugnis des Schularztes zur Speicherung von Daten der Schulgesundheitspflege ist § 58 Abs. 2 Buchst. a der Dritten DVO zum Gesetz über die Vereinheitlichung des Gesundheitswesens zu entnehmen. Unklar ist indessen, ob und ggf. in welchem Umfang eine Auskunftspflicht der Betroffenen bei Schulgesundheitsuntersuchungen besteht. Dieses Problem braucht jedoch nicht vertieft zu werden, weil die Gesundheitsämter schon jetzt darauf verzichten, die Schulgesundsheitsuntersuchungen zwangsweise durchzusetzen. Dies ist deshalb möglich, weil Verweigerungsfälle selten sind und der Effekt einer zwangsweise durchgesetzten Untersuchung gering wäre. Für die Übergangszeit bis zum Erlaß normenklarer Regelungen in einem Gesundheitsdienstgesetz sieht die DSK jedenfalls in der Erhebung von Anamnesedaten auf freiwilliger Grundlage – nach detaillierter Aufklärung der Eltern – eine datenschutzrechtlich tragfähige Lösung.

Die mit der Anwendung verbundenen Datensicherungsprobleme sind – auch im PC-Bereich – grundsätzlich lösbar. Unvermeidbar ist freilich, daß für die Anschaffung der notwendigen Hardware- und Softwaresicherungen zusätzliche Kosten entstehen.

Im einzelnen forderte die DSK:

- Zugriffsschutz, auch auf der Ebene des Laptop, durch Einführung eines Paßwortsystems; Protokollierung von Benutzeraktivitäten, insbesondere von Kopiervorgängen,
- Online-Verschlüsselung der Festplatte, Kopierschutz durch Verschlüsselung,
- anonymisierte Datenspeicherung im PC des Gesundheitsamtes (Ordnungsnummer, Referenzliste),
- Ausschluß des Zugriffs zur Betriebssystemebene,
- Bootschutz zum Diskettenlaufwerk.

Zu beanstanden war gegenüber dem Ministerium, daß der Probebetrieb mit Echtdaten aufgenommen wurde, obwohl die technischen und organisatorischen Datensicherungsmaßnahmen nach § 9 Abs. 1 LDatG noch nicht realisiert waren und auch keine Dienstanweisung nach § 9 Abs. 2 LDatG existierte.

9.5 Ergebnisse örtlicher Feststellungen bei einem Gesundheitsamt

In den Gesundheitsämtern werden Daten von außerordentlich hoher Sensitivität verarbeitet. Abgesehen von dem unter Tz. 9.4 dargestellten Verfahren geschieht dies in herkömmlicher Form, also durch Erfassung und Aufzeichnung in Akten, Karteien, Listen usw. Die Sicherung dieser Informationsbestände ist nicht nur ein Gebot, das aus der Verschwiegenheitspflicht der Ärzte und ihres Hilfspersonals, von Sozialarbeitern usw. herzuleiten ist, es ergibt sich auch aus den allgemeinen Pflichten öffentlich Bediensteter.

Es ist ohne Zweifel sehr wichtig, daß Akten, Karteien und andere Aufzeichnungen unter Verschluß gehalten werden, nicht minder wichtig ist aber die Einbindung aller Einzelmaßnahmen in ein organisatorisches Konzept, das die Zuständigkeiten und Verantwortlichkeiten klarstellt und verbindliche Handlungsanweisungen umfaßt.

Die DSK hat im Rahmen einer Prüfung bei einem Gesundheitsamt Feststellungen getroffen, die sicherlich nicht die Situation in allen Ämtern kennzeichnen, die aber dennoch von allgemeinem Interesse sein dürften. Aus diesem Grunde werden Berichtsauszüge nachfolgend wörtlich wiedergegeben.

„a) Der Organisationsplan des Gesundheitsamtes ist sowohl im personellen wie auch im funktionsbeschreibenden Teil inaktuell.

Da beim Gesundheitsamt Informationen von hoher Sensibilität erhoben und verarbeitet werden ist es unerläßlich, daß sowohl bei den Bediensteten wie auch bei den aufsichtsführenden Stellen jederzeit Klarheit darüber besteht, wer für welche Aufgabenbereiche zuständig ist und wie die Verantwortlichkeiten in datenschutzrechtlicher Hinsicht verteilt sind.

b) Schriftliche Anordnungen über die Datensicherung und die Zugriffsbefugnisse auf die jeweiligen Gesundheitsamtsakten konnten nicht vorgelegt werden. In einer Behörde, in der fast alle Vorgänge der ärztlichen Schweigepflicht und unbefugte Offenbarungen der Strafandrohung des § 203 StGB unterliegen, ist es unerläßlich, daß schriftliche Regelungen der genannten Art getroffen werden.

c) Die Akten des Gesundheitsamtes sind – jedenfalls zu einem Teil – in offenen Regalen für alle Bediensteten zugänglich abgelegt bzw. abgestellt. Diese Form der Aktenführung kann im Blick auf den sensiblen Akteninhalt nicht akzeptiert werden. Es ist erforderlich, daß die Akten in verschließbaren Schränken aufbewahrt werden. Angemessen wären Metallschränke. Ferner muß ein Aktenverzeichnis und ein Nachweis über den jeweiligen Verbleib der Akten geführt werden.

d) Die Altaktei des Gesundheitsamtes befindet sich in Kellerräumen. Eine Stichprobenprüfung ergab, daß die Verwaltungsvorschrift über Aufbewahrungsfristen, Löschung und Abgabe ärztlicher Unterlagen der Gesundheitsämter vom 23. September 1982, MinBl. S. 502, nicht beachtet wird. Es war nicht feststellbar, ob regelmäßige Prüfungen bezüglich der Löschung und Abgabe der Materialien stattfinden.

Wir bitten, die gesamten in der Altaktei vorhandenen Materialien unter Zugrundelegung der genannten Verwaltungsvorschriften zu überprüfen, die Vernichtung durchzuführen oder die Übernahme durch das Landesarchiv einzuleiten.

e) Die Altakten waren in den Kellerräumen auf Regalen abgelegt. Auch Karteien – beispielsweise eine Geschlechtskrankenkartei mit äußerst empfindlichem Inhalt – waren nicht zusätzlich geschützt. Diese Form der Aufbewahrung genügt nicht den Anforderungen. Erforderlich sind verschließbare Schränke, für besonders schutzbedürftige Akten und Karteien Stahlschränke.

f) In den Kellerräumen befanden sich auch Materialien, die im Zusammenhang mit der Nebentätigkeit eines früheren Leiters des Gesundheitsamtes entstanden sind. Die weitere Aufbewahrung dieser Materialien in der Altaktei des Gesundheitsamtes ist nicht zulässig. Die Akten sind zu vernichten."

Die Richtigkeit der von der DSK getroffenen Feststellungen wurde von den zuständigen Aufsichtsbehörden im wesentlichen bestätigt. Sämtliche Dienststellen der Gesundheitsverwaltung im Lande wurden unterrichtet und aufgefordert, die Datensicherungsmaßnahmen zu überprüfen und in eigener Zuständigkeit das Erforderliche zu veranlassen. Das Ministerium prüft z. Z. die Notwendigkeit und Zweckmäßigkeit des Erlasses einer Dienstanweisung über den Datenschutz in den Gesundheitsämtern.

9.6 Datenschutz im Krankenhaus

9.6.1 Allgemeines

In ihrem 11. Tätigkeitsbericht gab die DSK eine Darstellung der Neuordnung des Datenschutzes im Krankenhausbereich und im Maßregelvollzug (Tz. 9.2). Sie begrüßte die gesetzgeberische Initiative, die zu einer im wesentlichen einheitlichen Rechtssituation für alle Krankenhäuser in öffentlicher und privater Trägerschaft führte. Entsprechend der Ermächtigung in § 38 hat die Evangelische Kirche im Rheinland am 1. September 1988 eine Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern erlassen (veröffentlicht im Amtsblatt der Ev. Kirche im Rheinland S. 261), die für ihren Anwendungsbereich den Regelungen der §§ 36 und 37 Landeskrankenhausgesetz vorgeht. In Kernfragen des Patientendatenschutzes stimmen diese Regelungen indessen mit den Landeskrankenhausgesetz überein. Für die Krankenhäuser in der Trägerschaft der übrigen Landeskirchen und der Katholischen Kirche sind entsprechende Verordnungen in Vorbereitung.

Die Landesregierung hat dem Landtag in Ausführung des Beschlusses vom 13. November 1986 einen Bericht über den Datenschutz im Krankenhausbereich erstattet, der sich weitgehend auf eine bei den Krankenhausträgern durchgeführte Erhebung stützt (Drucksache 11/2565). Dieser Bericht zeichnet das Bild eines funktionierenden Datenschutzes im Krankenhausbereich: Die den Datenschutz betreffenden Regelungen des Landeskrankenhausgesetzes würden von den Krankenhausträgern sowie

von den mit der Erhebung und Verarbeitung von Daten befaßten Krankenhäusern angenommen und beachtet. Insbesondere der Umstand, daß nur selten Patientendaten aufgrund der Ausnahmebestimmungen ohne die Einwilligung der Betroffenen weitergeleitet würden, zeige den hohen Stellenwert, der von Krankenhausträgern und Krankenhausverwaltungen der Entscheidungsbefugnis der Patienten über den Umgang mit den sie betreffenden Daten beigemessen würde. Andererseits führten die Datenschutzregelungen des Landeskrankenhausgesetzes nicht zur Behinderung notwendiger Erhebungen. Dies liege auch an der Bereitschaft der meisten Patienten, in die gesetzmäßige und sinnvolle Nutzung der sie betreffenden Daten einzuwilligen.

Nach Auffassung der DSK fordert die Situation des Datenschutzes im Krankenhausbereich eine etwas differenziertere Betrachtung. Ohne Zweifel besteht in vielen Krankenhäusern noch keine Klarheit über die Folgerungen, die aus den Datenschutzbestimmungen des Gesetzes zu ziehen sind. Ein Beispiel hierfür ist die Tatsache, daß es in mehreren Krankenhäusern fast zwei Jahre dauerte, bis ein Datenschutzbeauftragter bestellt war, wie es § 36 Abs. 8 Landeskrankenhausgesetz fordert. Noch immer umfaßt der Aufnahmedatensatz beispielsweise das Merkmal „Konfession", das zur Erstellung der sog. Pfarrerlisten führt, aber nur auf der Grundlage der Patienteneinwilligung erhoben werden darf, und noch immer besteht in den Krankenhäusern weitgehende Unklarheit darüber, unter welchen Bedingungen beispielsweise Daten zwischen den einzelnen Abteilungen und Kliniken sowie an Stellen außerhalb des Krankenhauses übermittelt werden dürfen.

Die DSK zweifelt jedenfalls nicht daran, daß noch erhebliche Vollzugsdefizite bestehen, die als solche noch nicht genügend erkannt wurden.

9.6.2 Erfahrungsaustausch mit den Krankenhaus-Datenschutzbeauftragten

Die externe Datenschutzkontrolle für die Krankenhäuser im öffentlichen Bereich – mit Ausnahme der Krankenhäuser in kirchlicher Trägerschaft – obliegt der DSK. Im Blick auf die Bedeutung des Patientendatenschutzes hat der Gesetzgeber aber noch ein weiteres getan: Er hat durch § 36 Abs. 8 Landeskrankenhausgesetz die Bestellung von Krankenhausdatenschutzbeauftragten als interne Kontroll- und Beratungsorgane verbindlich vorgeschrieben.

Das Bestreben der DSK ist darauf gerichtet, die Arbeit der Krankenhausdatenschutzbeauftragten zu unterstützen. Sie hat aus diesem Grunde im Juni dieses Jahres die Beauftragten der ihrer Kontrollzuständigkeit unterliegenden Krankenhäuser zu einem Erfahrungsaustausch eingeladen. Die Veranstaltung fand ein lebhaftes Echo und soll, unter wechselnder Federführung, wiederholt werden.

9.6.3 Informationsschrift „Datenschutz im Krankenhaus"

Mit der Herausgabe eines Hefts 4 „Datenschutz im Krankenhaus" im Rahmen der Schriftenreihe „Informationen zum Datenschutz" will die DSK allen im Krankenhausbereich mit Datenschutzfragen befaßten Personen Hilfestellungen für die tägliche Arbeit geben. Die Schrift ist so praxisnah gestaltet, wie dies aus derzeitiger Sicht möglich ist; es ist vorgesehen, die Erfahrungen bei der Anwendung der datenschutzrechtlichen Vorschriften des Landeskrankenhausgesetzes kontinuierlich einzuarbeiten und damit den Wert künftiger Auflagen zu erhöhen.

Das Heft kann kostenlos von der Geschäftsstelle der DSK bezogen werden.

9.7 Perinatologische Basiserhebung

Im Rahmen des Projekts „Perinatologische Basiserhebung" werden von einer bei der Kassenärztlichen Vereinigung Trier gebildeten Dokumentationszentrale seit dem Jahre 1985 Daten über den Gesundheitszustand von Schwangeren und den Verlauf von Entbindungen erfaßt und ausgewertet. Die DSK berichtete hierüber bereits im Jahre 1985 (10. Tätigkeitsbericht, Tz. 9.3). Das datenschutzrechtliche Kernproblem war die Erhebung und die Auswertung außerordentlich empfindlicher Informationen, wie z. B. Schwangerschaftsabbrüche, Drogen- und Alkoholabhängigkeit, psychosoziale Belastungen, in einer nicht vollständig anonymisierten Form. Die DSK konnte sich seinerzeit mit ihrer Forderung, entweder die Zustimmung der betroffenen Frauen zur Datenübermittlung und -verarbeitung einzuholen oder die Daten weitergehend – insbesondere durch den Verzicht auf die genaue Kennzeichnung des Wohnortes – zu anonymisieren, nicht durchsetzen. Als Teilerfolg war immerhin die Zusicherung der Kassenärztlichen Vereinigung anzusehen, daß anstatt der ursprünglich vorgesehenen vierstelligen Postleitzahl zur Kennzeichnung des Wohnortes nur eine dreistellige Postleitzahl verwendet werde. Bei der Erfassung einer auf zwei Stellen reduzierten Postleitzahl sei, so erklärte die Kassenärztliche Vereinigung Trier gegenüber der DSK, dem „daraus resultierenden Ergebnis keine bedeutende Effizienz beizumessen". Man werde ggf. auf die Durchführung der Perinatalerhebung verzichten.

Im Dezember 1988 fand eine datenschutzrechtliche Prüfung der Anwendung in der Dokumentationszentrale der Kassenärztlichen Vereinigung Trier statt. An dieser Prüfung beteilige sich auch der Saarländische Datenschutzbeauftragte, dessen Kontrollzuständigkeit wegen der Verarbeitung von Daten saarländischer Kliniken ebenfalls begründet ist.

Die Erhebungsbogen wurden stichprobenweise überprüft. Dabei ergab sich, daß ausnahmslos eine vierstellige Postleitzahl eingetragen, der Wohnort der betroffenen Frauen also exakt gekennzeichnet war. Für die weitere Verarbeitung wurden aber nur drei Stellen erfaßt. Gleichwohl war die Identifizierungsmöglichkeit der einzelnen Berichtsfälle durch die genaue Kennzeichnung des Wohnortes signifikant erhöht.

Ferner ergab die Prüfung, daß die erfaßten dreistelligen Postleitzahlen in die Auswertung der Daten nicht einbezogen wurden, mit anderen Worten, die Postleitzahl spielte für die Gewinnung von Ergebnissen aus der Perinatalen Basiserhebung überhaupt keine Rolle. Nimmt man die frühere Erklärung der Kassenärztlichen Vereinigung wörtlich, so ist den durch die Verarbeitung gewonnenen Ergebnissen keine bedeutende Effizienz beizumessen und auf die Durchführung der Perinatalerhebung müßte eigentlich verzichtet werden.

Auch andere zunächst kontrovers behandelte Punkte, über die dann bei den Beratungen zwischen der DSK und Vertretern der Kassenärztlichen Vereinigung Trier im Jahre 1985 schließlich Einigkeit erzielt werden konnte, wurden nicht vereinbarungsgemäß realisiert. So erkannte die Kassenärztliche Vereinigung an, daß für die Datenverarbeitung ein Auftragsverhältnis zwischen den Entbindungseinrichtungen und der Dokumentationszentrale unter Verwendung eines Vertrages zu begründen sei, der im Detail mit der DSK abgestimmt wurde. Dieser Vertrag fand, wie die örtlichen Feststellungen ergaben, keine Verwendung.

Einvernehmen war auch darüber erzielt worden, daß die als Identifizierungsmerkmal besonders geeignete Geburtsnummer, die von den Kliniken vergeben wird, nach Abschluß der Plausibilitätsprüfung in der Dokumentationszentrale gelöscht wird. Dies ist indessen ebenfalls nicht geschehen.

Die Ergebnisse der örtlichen Feststellungen wurden in einer DSK-Sitzung im März dieses Jahres mit Vertretern des MUG erörtert. Die DSK erhielt die Zusage, daß nach Klärung unter Einbeziehung der Wissenschaftlichen Begleitkommission, der Landesärztekammer und der Kassenärztlichen Vereinigung Trier Stellung genommen und über das Veranlasste berichtet werde. Die Stellungnahme ist nach Erinnerung im November eingegangen. Sie widerlegt die Feststellungen der DSK in keinem Punkt.

9.8 AIDS

9.8.1 Allgemeines

Die Landesregierung hat wiederholt bekräftigt, daß sie die Möglichkeiten der AIDS-Bekämpfung ausschließlich im Bereich der Information, der Aufklärung, der Beratung und Vorbeugung sieht. Sie geht davon aus, daß z. Z. nach wie vor von freiwillig zu nutzenden Angeboten der Testung, Beratung und von sozialen Hilfen der verschiedensten Art eine größere Wirksamkeit bei der Eindämmung dieser Krankheit zu erwarten ist, als durch die Verschärfung seuchenrechtlicher Bestimmungen mit dem Ziel allgemeiner Zwangsmöglichkeiten. Für konkrete Einzelfälle, bei denen durch freiwillige Maßnahmen ein Schutz der Bevölkerung nicht erreichbar ist, stehen nach Auffassung der Landesregierung die für Zwangsmaßnahmen erforderlichen Möglichkeiten im Bundes-Seuchengesetz, im Strafrecht und in den Unterbringungsgesetzen der Länder in bisher ausreichendem Umfange zur Verfügung (vgl. AIDS-Bericht der Landesregierung, Drucksache 11/1392, S. 29).

Die Strategie der Landesregierung bei der AIDS-Bekämpfung deckt sich im wesentlichen mit der Haltung, die von der DSK in Fragen der ärztlichen Informationsverarbeitung und insbesondere hinsichtlich der Gewinnung epidemiologischer Daten eingenommen wurde. Die damit gewonnenen Erfahrungen begründen keinesfalls die Notwendigkeit, von diesem datenschutzrechtlich wünschenswerten Konzept abzugehen. Dies ist um so erfreulicher, als der Datenschutz mit seinen Forderungen nach Beachtung der Persönlichkeitsrechte durch freiwillige und anonymisierte Datenerhebung und -verarbeitung gelegentlich als Behinderung einer wirkungsvollen AIDS-Bekämpfung angesehen wurde.

9.8.2 HIV-Tests

Aufklärung, Beratung und Vorbeugung sind nach wie vor die wichtigsten Waffen im Kampf gegen AIDS. Eine zentrale Bedeutung haben dabei die sog. HIV-Tests, die kostenlos und, sofern der Proband dies wünscht, anonym durchgeführt werden.

Für die Akzeptanz dieser Tests ist von entscheidender Bedeutung, daß das Vertrauen in die strikte Wahrung der Anonymität besteht und erhalten bleibt. Die DSK hat deshalb mehrfach Vorschläge zur Verbesserung des Anonymisierungsverfahrens gemacht und ist gelegentlichen Hinweisen auf Mängel sofort nachgegangen. Sie hat indessen keine Verstöße festgestellt.

Vom MUG aufgegriffen wurde eine Empfehlung der DSK bezüglich der Codierung von Testbegleitzetteln. Die meisten Gesundheitsämter codierten in der Vergangenheit unter Verwendung einer laufenden Nummer und einer zusätzlichen Buchstaben/Zahlenkombination, bestehend aus dem Anfangsbuchstaben des Vor- oder Nachnamens, dem Geburtsjahr oder sonsti-

gen Kennworten oder Zahlenangaben des Probanden. Diese Codierung erhöht zwar die Sicherheit der Zuordnung von Testergebnissen, weil sich der Proband in aller Regel an solche Chiffren leichter erinnert als an reine Zahlenangaben. In Ausnahmefällen kann eine solche Codierung aber zur Identifizierung geeignet sein.

Das Ministerium ordnete an, daß bei der Codierung nur noch eine laufende Nummer in Verbindung mit der Jahreszahl der Testung verwendet wird.

Eine weitere Empfehlung der DSK betraf die Aufbewahrung von Befundduplikaten bei nicht anonymer Testung. Das Ministerium hält die Aufwahrung dieser Duplikate aus Gründen der ärztlichen Dokumentationspflicht und auch deshalb für erforderlich, weil die Befunde später angefochten werden oder in Gerichtsverfahren Bedeutung erlangen könnten. Es wies die Gesundheitsämter aber an, die Probanden vor der Entscheidung über die Art des durchzuführenden Tests – anonym oder personenbezogen – darüber zu informieren, daß die Untersuchungsbefunde bei personenbezogenen Tests aufbewahrt werden.

9.8.3 Zwangsweise ärztliche Untersuchung von Asylbewerbern

Asylbewerber wurden in der Vergangenheit routinemäßig wie folgt untersucht:

- Allgemeine körperliche Inaugenscheinnahme;

- Untersuchung auf behandlungsbedürftige Tuberkulose der Atmungsorgane; Lues; Hepatitis B; HIV-Antikörper, wenn ein positiver HBs- und/oder Luesbefund vorlag; weitere Erkrankungen, insbesondere Salmonellen/Schigellen, soweit dies aufgrund der epidemiologischen Situation des Herkunftslandes angezeigt war.

Bereits im vorangegangenen Berichtszeitraum hatte die DSK gegenüber dem MUG die Frage problematisiert, ob eine ausreichende gesetzliche Grundlage für die Durchführung dieser routinemäßigen, vom Einverständnis der Betroffenen nicht abhängigen ärztlichen Untersuchungen der Asylbewerber vorhanden sei (vgl. 12. Tätigkeitsbericht; Tz. 8.3).

Der Bundesbeauftragte für den Datenschutz unterstützte in einem Schreiben an den Bundesminister des Innern die auf die Schaffung einer einwandfreien gesetzlichen Grundlage für die Untersuchungen gerichteten Bestrebungen der DSK.

Auch das MUG erkannte schließlich an, daß weder dem Bundesseuchengesetz noch dem Ausländergesetz eine Rechtsgrundlage für die obligatorische ärztliche Untersuchung zu entnehmen ist. Sie kann lediglich im Einzelfall nach § 20 Abs. 2 Asylverfahrensgesetz dem Asylbewerber zur Auflage gemacht werden.

Eine auf die Schaffung einer Rechtsgrundlage für obligatorische Gesundheitsuntersuchungen aller Asylbewerber gerichtete Initiative des Ministeriums in der Arbeitsgemeinschaft der Länder-Medizinalbeamten (AGLMB) blieb bisher ohne konkretes Ergebnis. Die Mehrheit der Länder sprach sich für die Durchführung der Untersuchungen auf der Grundlage von Angebotsuntersuchungen – also gegen obligatorische Untersuchungen – aus. Von einer Minderheit wurde allerdings eine gesetzliche Regelung auch für Angebotsuntersuchungen aus Gründen der Rechtsklarheit für „notwendig bzw. wünschenswert" gehalten. Zur Vorbereitung eines Beschlußvorschlags sollte die Problematik vertieft in einer Arbeitsgruppe beraten werden. Ein Ergebnis dieser Beratungen wurde bisher nicht bekannt.

Die DSK verbleibt bei ihrer Auffassung, daß eine obligatorische Untersuchung von Asylbewerbern nicht zulässig ist. Die Auflage, sich einer Untersuchung zu unterziehen, kann jedoch im Einzelfall aus begründetem Anlaß auf § 20 Abs. 2 Asylverfahrensgesetz gestützt werden. Sofern aus gesundheitsärztlicher Sicht routinemäßige Untersuchungen für erforderlich gehalten werden, muß die Forderung nach Schaffung gesetzlicher Eingriffsgrundlagen aufrecht erhalten werden. Durch „Angebotsuntersuchungen" auf der fragwürdigen Grundlage einer Scheinfreiwilligkeit kann das Problem jedenfalls nicht gelöst werden.

10 Kultusbereich

10.1 Schulbereich

10.1.1 Regelung der Datenverarbeitung in den Schulordnungen

Im 10. Tätigkeitsbericht wurde dargestellt, welche datenschutzrechtlichen Regelungen in das Schulgesetz (auf Initiative der DSK) aufgenommen wurden (Tz. 7.1, S. 22 ff). In dem im Juli 1985 in Kraft getretenen 3. Abschnitt des Schulgesetzes, der sich mit der Erhebung und Verarbeitung von Daten befaßt, wurde der Kultusminister ermächtigt und verpflichtet, Regelungen über die zulässigen Verwendungszwecke beim Einsatz automatisierter Verfahren sowie die dabei erforderlichen Datensicherungsmaßnahmen und Aufbewahrungsfristen durch Rechtsverordnung zu schaffen. Dabei sind auch die bei der Aufnahme in die Schule, beim Schullaufbahnwechsel und bei vergleichbaren Anlässen zu erhebenden oder zu übermittelnden Daten zu be-

stimmen (§ 54 a Abs. 4 SchulG). Diesem Auftrag ist der Kultusminister inzwischen durch Ergänzungen einiger Schulordnungen – leider noch nicht für alle Schularten – nachgekommen: Zunächst wurde die Grundschulordnung um einen 8. Abschnitt ergänzt, der sich mit der Erhebung von Daten und dem Datenschutz befaßt (SchulO für die öffentlichen Grundschulen vom 21. Juli 1988, BS 223-1-37). Auch die schulartübergreifende SchulO wurde entsprechend erweitert (um einen 11. Abschnitt, Erhebung von Daten, Datenschutz: SchulO für die öffentlichen Hauptschulen, Realschulen, Gymnasien und Kollegs vom 13. Juni 1989, BS 223-1-35). Außerdem erhielten die Schulordnungen Vorschriften über die bei der Anmeldung zu erhebenden Daten (§ 1 GrundschulO, § 10 Abs. 3 schulartübergreifende SchulO). In den Schulordnungen sind darüber hinaus schon herkömmlich mehrere Vorschriften mit datenschutzrechtlichem Gehalt enthalten, die die Erhebung oder Übermittlung von Daten regeln.

Die DSK wurde frühzeitig an der datenschutzrechtlichen Ergänzung der Schulordnungen beteiligt. Ihre Vorschläge und Anregungen wurden weitgehend berücksichtigt. Unter der Überschrift „Erhebung von Daten, Datenschutz" enthalten die Schulordnungen nunmehr folgende zusätzliche Regelungen:

10.1.1.1 Zulässigkeit der automatisierten Speicherung von Schülerdaten

Grundregel ist, daß alle zulässigerweise durch die Schule erhobenen Daten eines Schülers auch automatisiert verarbeitet werden dürfen. Ausgenommen von der Zulässigkeit der automatisierten Speicherung sind jedoch Schülerdaten, die durch schulärztliche, schulpsychologische und ähnliche Maßnahmen (gem. § 52 Abs. 3 SchulG) erhoben worden sind sowie Schülerdaten, die anläßlich von Ordnungsmaßnahmen angefallen sind. Diese dürfen nicht automatisiert verarbeitet werden (§ 52 Abs. 2 GrundschulO, § 76 Abs. 2 schulartübergreifende SchulO).

Für die automatisiert gespeicherten Schülerdaten ist eine bedeutsame Zweckbindungsregelung geschaffen worden: Sie dürfen nur für die Verwaltungsaufgaben der Schule verwendet werden. Diese Zweckbindung hat zwei Auswirkungen:

- Schülerdaten, die für Verwaltungsaufgaben der Schule nicht benutzt werden können oder die für Verwaltungsaufgaben der Schule unerheblich sind, dürfen nicht automatisiert gespeichert werden.

- Außerdem begrenzt diese Zweckbindung auch die Benutzung der zulässigerweise gespeicherten automatisierten Daten: andere als Schulverwaltungszwecke dürfen mit ihnen nicht erfüllt werden.

Für den Einsatz von Textautomaten wurde eine besondere Regelung getroffen: diese dürfen umfassend eingesetzt werden, auch zur Verarbeitung von Schülerdaten, die ansonsten nicht automatisiert gespeichert werden dürfen, wenn nach Erstellung der jeweiligen Texte eine sofortige Löschung erfolgt (§ 52 Abs. 2 S. 2 und 3 GrundschulO, § 76 Abs. 2 schulartübergreifende SchulO).

10.1.1.2 Nutzung privater DV-Geräte durch Lehrer zu dienstlichen Zwecken

Für die Nutzung privater DV-Geräte für dienstliche Zwecke , die in der Praxis bedeutsam ist, und die in anderen Bundesländern völlig untersagt ist (z. B. in Baden-Württemberg, Bremen), enthalten die Schulordnungen Vorgaben, die diesen Einsatz zulassen. Maßgeblich für die Zustimmung der DSK dazu war, daß es nicht vertretbar erschien, die Nutzung der Technik in diesem Bereich grundsätzlich zu untersagen, ohne daß dafür ein zwingender Grund besteht. Auch angesichts der Akzeptanzprobleme bei allen Betroffenen erschien es der DSK angemessen, bestimmte einengende Regelungen vorzuschlagen, die den Einsatz dieser Geräte datenschutzverträglich gestalten. Die Alternative einer einfachen, radikalen Lösung, die in der Praxis auf das völlige Unverständnis einer engagierten Lehrerschaft stieße, erschien der DSK ungeeignet. Schülerdaten dürfen also in privateigenen PC der Lehrer unter folgenden Voraussetzungen automatisiert gespeichert werden:

- Die fraglichen Daten müssen erforderlich sein, damit der Lehrer die ihm durch das Gesetz zugewiesenen schulbezogenen Aufgaben erfüllen kann;

- diese Daten dürfen ausschließlich für schulische Verwaltungsaufgaben, insbesondere für die Erstellung von Zeugnissen und für die schulische Korrespondenz, genutzt werden;

- der Einsatz der dienstlichen Datenverarbeitung auf dem privaten DV-Gerät ist vom Lehrer dem Schulleiter anzuzeigen; Voraussetzung ist weiter, daß dieser den Einsatz genehmigt;

- Voraussetzung der Genehmigung ist, daß der betroffene Lehrer eine Einverständniserklärung erteilt, daß das DV-Gerät durch die zuständigen Stellen (Schulleitung, Schulbehörden, DSK) kontrolliert werden kann;

– der betroffene Lehrer hat die erforderlichen Datensicherungsmaßnahmen (z. B. Abschließbarkeit des Gerätes, Gewährleistung der sicheren Verwahrung der Datenträger) einzurichten.

Diese Anforderungen ergeben sich aus § 54 a Abs. 1 SchulG in Verbindung mit § 76 Abs. 2 S. 1 und Abs. 3 der schulartübergreifenden SchulO bzw. mit § 52 Abs. 2 S. 1 und Abs. 3 GrundschulO.

10.1.1.3 Datensicherungsanforderungen

Neu ist, daß nunmehr in die Schulordnungen eine Regelung für Datensicherungsmaßnahmen auch bei manueller Speicherung (etwa in Schülerakten) getroffen wurde: Für personenbezogene Daten, die nicht automatisiert verarbeitet werden, ist sicherzustellen, daß sie nur denen zugänglich gemacht werden, die sie für die Erfüllung ihrer dienstlichen Aufgaben benötigen (§ 53 Abs. 1 S. 2, GrundschulO, § 77 Abs. 1 S. 2 schulartübergreifende SchulO). Damit wird deutlich gemacht, daß auch solche Unterlagen grundsätzlich schutzbedürftig sind.

Für die automatisierte Datenverarbeitung verweisen die Schulordnungen auf das allgemeine Datenschutzrecht (Landesverordnung über technische und organisatorische Datenschutzanforderungen nach § 9 des LDatG, BS 204-1-1).

10.1.1.4 Zur Löschung von Schüler- und Elterndaten

Bedeutsame Regelungen sind auch für die Löschung von Daten aufgenommen worden: Personenbezogene Daten in automatisierten Dateien sind zu löschen, sobald ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist, spätestens jedoch ein Jahr nachdem der Schüler die Schule verlassen hat. Hiervon ausgenommen sind die Namen und Aktennachweise, die bis zur Vernichtung der Akte automatisiert gespeichert werden dürfen. Damit ist § 13 LDatG in begrüßenswerter Weise für die schulischen Verhältnisse konkretisiert worden.

Für Daten in Akten und in nicht automatisierten Dateien ist folgende Regelung getroffen worden: Diese sind ein Jahr, nachdem der Schüler die Schule verlassen hat, zu sperren. Sie dürfen von diesem Zeitpunkt an nicht mehr genutzt werden, es sei denn, daß dies zur Behebung einer bestehenden Beweisnot, aus sonstigen, im überwiegenden Interesse der Schule liegenden Gründen oder im rechtlichen Interesse Dritter unerläßlich ist oder der Betroffene eingewilligt hat (§ 53 Abs. 2 und 3 GrundschulO, § 77 Abs. 2 und 3 schulartübergreifende SchulO).

Schließlich ist in den Schulordnungen jetzt auch eine Rechtsgrundlage für die Anordnung des Kultusministeriums über die Aufbewahrung, Aussonderung, Archivierung und Vernichtung des amtlichen Schriftgutes enthalten. Diese Anordnung war bislang von der DSK unter verschiedenen Gesichtspunkten kritisiert worden (vergl. 10. Tätigkeitsbericht, Tz. 10.1.4 c, S. 43). So hatte die DSK gerügt, daß dieses Rundschreiben auch Schriftgut und Datenträger betrifft, die personenbezogene Daten von Schülern, Eltern oder Lehrern enthalten, ohne daß die gesetzlichen Vorgaben (§ 13 LDatG und § 54 a Abs. 4 SchulG) beachtet worden waren. Nunmehr ist durch die vorrangigen Regelungen der Schulordnungen den gesetzlichen Anforderungen entsprochen. Das Rundschreiben behält also nur im Rahmen dieser Anforderungen Wirksamkeit und hat damit nur noch im Bereich der manuellen Speicherungen personenbezogener Daten Bedeutung. Zudem sehen die Schulordnungen ausdrücklich vor, dies durch Verwaltungsvorschrift zu regeln (§ 53 Abs. 4 GrundschulO, § 77 Abs. 4 schulartübergreifende SchulO).

10.1.1.5 Besondere Übermittlungsregelungen

Die Schulordnungen enthalten weiter Regelungen über den Austausch von Elternadreßlisten zu Beginn eines Schuljahres zwischen den betroffenen Eltern einer Klasse; sie regeln die Zulässigkeit der Angabe bestimmter Basisdaten von Schülern und Eltern in Dokumentationen und Jahresberichten der Schule; schließlich regeln sie die Übermittlung von Schüler- und Lehreradreßdaten an ehemalige Schüler zur Organisation von Schülertreffen (§ 52 Abs. 4 – 6 GrundschulO, § 77 Abs. 5 – 7 schulartübergreifende SchulO). Diese Regelungen sind aus datenschutzrechtlicher Sicht als Ausdruck einer angemessenen Interessenabwägung in diesem Bereich anzusehen.

10.1.2 Einzelfragen zum Umgang mit Schülerdaten in der Schule

10.1.2.1 Speicherung in Klassenbüchern

Aufgrund von Eingaben hatte sich die DSK mit der Frage zu befassen, in welchem Umfang Schüler- und Lehrerdaten in Klassenbüchern gespeichert werden dürfen. In die schulartübergreifende Schulordnung ist nunmehr eine ausdrückliche Regelung aufgenommen worden. Danach dürfen in Klassenbüchern und Kursbüchern eingetragen werden:

– Namen und Geburtsdatum der Schüler,

– Teilnahme an Schulveranstaltungen,

– Vermerk über unentschuldigtes und entschuldigtes Fernbleiben und über Beurlaubungen,

– erzieherische Einwirkungen gem. § 83 Abs. 1 SchulO,

– Namen und Anschrift der Eltern,

– Angaben zur Herstellung des Kontakts in Notfällen.

Die DSK hat eine entsprechende Regelung auf Gesetzesebene zwar nicht für unabdingbar erforderlich gehalten, sie begrüßt jedoch die damit erreichte Klarstellung der Rechtslage.

10.1.2.2 Antragsverfahren für Lernmittelgutscheine

Mitte des Jahres 1988 hat die Umstellung des Verfahrens zur Erteilung von Lernmittelgutscheinen lebhafte öffentliche Proteste hervorgerufen, die auch datenschutzrechtliche Aspekte dieses Verfahrens betrafen. Auf Beschluß des Landtags war die Erteilung von Lernmittelgutscheinen für die Sekundarstufe 1 in gleicher Weise einkommensabhängig gestaltet worden, wie dies bislang nur für die Sekundarstufe 2 der Fall gewesen war. Damit wurde es für eine große Zahl von Eltern erforderlich, Einkommensangaben zu machen, um entsprechende Lernmittelgutscheine zu erhalten. In diesem Zusammenhang hat sich eine größere Zahl von datenschutzrechtlichen Fragen gestellt:

So wurde von betroffenen Eltern gerügt, daß die Klassenlehrer über ihre Einkommensverhältnisse unterrichtet würden; es wurde weiter beanstandet, daß die Angaben in dem Antrag auf Erteilung von Lernmittelgutscheinen innerhalb der Klasse und innerhalb der Schule einem unüberprüfbar großen Personenkreis zur Kenntnis gelangen konnten; auch die Vergabe der Lernmittelgutscheine, die Rückschlüsse auf die Einkommenssituation der Bezugsberechtigten zuläßt, wurde insofern beanstandet, als sie „klassenöffentlich" erfolgte.

Es kam hinzu, daß die Schulen teilweise verlangt haben, das Antragsformular auf jeden Fall ausgefüllt abzugeben, auch wenn von vornherein klar war, daß aufgrund der Höhe der Einkünfte kein Anspruch auf Lernmittelgutscheine bestand: Damit wollten einige Lehrer sicherstellen, daß wirklich alle Eltern die entsprechenden Anträge zur Kenntnis nehmen würden. Gleichzeitig war damit allerdings eine überflüssige Kenntnisnahme von Daten verbunden, die von den Betroffenen als sensibel angesehen worden sind.

Die DSK hat erreicht, daß für das Verfahren des darauffolgenden Jahres Modalitäten der Antragsentgegennahme, Bearbeitung und Lernmittelgutscheinausgabe eingeführt wurden, die den vorgetragenen Bedenken Rechnung getragen haben.

10.1.2.3 Anwesenheit von Eltern im Schulunterricht

Im Zuge der Neufassung der Schulordnungen wurde sowohl in der Grundschulordnung wie in der schulartübergreifenden Schulordnung den Eltern die Möglichkeit gegeben, am Unterricht ihrer Kinder teilzunehmen (§ 14 Abs. 5 GrundschulO, § 9 Abs. 2 schulartübergreifende SchulO). Ein Elternbeiratsvorsitzender hat in diesem Zusammenhang gegenüber der DSK die Frage aufgeworfen, ob durch eine entsprechende Teilnahme von Eltern am Unterricht nicht unzulässig in das informationelle Selbstbestimmungsrecht der jeweiligen Mitschüler eingegriffen wird. Die DSK geht davon aus, daß durch die Anwesenheit von Eltern im Schulunterricht Informationen über alle Schüler der entsprechenden Klasse an die anwesenden Eltern gelangen. Insofern liegt ein Eingriff in das informationelle Selbstbestimmungsrecht vor. Die DSK hat jedoch darauf hingewiesen, daß dieser Eingriff aufgrund einer gesetzlichen Regelung (den zitierten Vorschriften der SchulO) erfolgt, die sowohl dem Gebot der Normenklarheit wie der Verhältnismäßigkeit entspricht. Das Ziel der Schulordnungen, ein gemeinsames Erziehungskonzept von Schule und Eltern zu realisieren und eine partnerschaftliche Zusammenarbeit zu erreichen, rechtfertigt eine entsprechende Regelung.

10.1.2.4 Datenübermittlung zum Zweck der Schulpflichtüberwachung

Aufgrund der Anfrage einer betroffenen Stadtverwaltung hat die DSK die Datenübermittlungen zwischen dem Melderegister und schulischen Stellen (Schulträgern und Schulen sowie Bezirksregierungen) untersucht und zum Gegenstand von Besprechungen mit den zuständigen Ressorts (ISM und KM) gemacht. Es hat sich ergeben, daß die gesetzlich vorgesehenen Datenübermittlungen (in § 7 Meldedatenübermittlungsverordnung – MeldDÜVO –) vom Melderegister an die Bezirksregierung zum Zweck der Schulpflichtüberwachung und der Zuordnung der schulpflichtigen Kinder an die jeweils zuständigen Schulen weder praktiziert werden noch sinnvoll sind. Die sinnvolle Verfahrensweise, daß entsprechende Daten von den Melderegistern an die jeweiligen Schulämter der Schulträger gelangen, damit dort aufgrund der örtlichen Kenntnisse die genannte Zuordnungsfunktion erfüllt werden kann, ist aber nach dem Wortlaut der maßgeblichen Vorschriften nicht zugelassen.

Die DSK hat deshalb empfohlen, bei nächster Gelegenheit § 7 MeldedatenübermittlungsVO – MeldDÜVO – zu ändern und zu bestimmen, daß die Meldedaten der Kinder an die Schulämter zu übermitteln sind. Die DSK geht bezüglich der z. Z. geltenden Rechtslage davon aus, daß die Schulämter bei der Zuordnung der Schüler zu den einzelnen Schulen im Auftrag der jeweiligen Bezirksregierung tätig werden. Dies hat sie im Hinblick auf §§ 2,59 SchulG zumindest für eine Übergangsfrist als zulässig angesehen.

10.1.2.5 Musterdienstanweisung für die automatisierte Datenverarbeitung in Schulen und Studienseminaren

Das Kultusministerium beabsichtigt, eine Musterdienstanweisung für die automatisierte Verarbeitung personenbezogener Daten in Schulen und staatlichen Studienseminaren im Amtsblatt zu veröffentlichen. Den betroffenen Stellen soll damit die in § 9 Abs. 2 LDatG geforderte Erstellung konkreter Dienstanweisungen erleichtert werden.

Die DSK hat in diesem Zusammenhang darauf hingewiesen, daß die wörtliche Übernahme eines allgemeinen Musters über die Einrichtung organisatorischer und technischer Maßnahmen zur Gewährleistung der datenschutzrechtlichen Anforderungen nach dem Landesdatenschutzgesetz grundsätzlich wohl nicht möglich ist. Entsprechende Sicherungsmaßnahmen, die in Dienstanweisungen festzulegen sind, müssen sich an der jeweils konkret eingesetzten Hard- und Software, der örtlichen Umgebung und den örtlichen Nutzungsbedingungen orientieren. Allgemein formulierte Dienstanweisungen werden – da sie alle denkbaren Aspekte umfassen müssen – einerseits zu umfangreich, andererseits aber an den örtlich wichtigen Punkten zu allgemein und damit zu nichtssagend sein. Außerdem besteht die Gefahr, daß das Bemühen um konkrete, angepaßte Sicherungsmaßnahmen durch die bloße wörtliche Übernahme einer allgemeinen Vorgabe gar nicht erst einsetzt. Die DSK hat deshalb angeregt, bei der Veröffentlichung des Musters auf die Problematik in geeigneter Form hinzuweisen und die Ergänzungsbedürftigkeit bezüglich der örtlichen Bedingungen hervorzuheben. Außerdem hat sie auf die Erforderlichkeit von Speicher- und Zugriffskontrollmaßnahmen bei der Vernetzung von PC auch innerhalb des Schulbereichs und bei der Nutzung einzelner Geräte zu unterschiedlichen Zwecken (z. B. Schulverwaltung und Unterricht) hingewiesen.

10.2 Hochschulbereich

10.2.1 Automatisierte Verarbeitung von Studentendaten

Im 11. Tätigkeitsbericht (Tz. 10.2.1) wurde dargestellt,daß nunmehr für die Erhebung und Verarbeitung von Studentendaten zu Verwaltungszwecken in den Hochschulgesetzen (HochschulG und FachhochschulG) Rechtsgrundlagen eingefügt worden sind, die den Erlaß von Einschreibeordnungen vorsehen, in denen konkretere Regelungen getroffen werden sollten.

Leider hat sich im Berichtszeitraum ergeben, daß die Hochschulen zum größten Teil nur sehr globale Regelungen in ihre Einschreibeordnungen aufgenommen haben, die den datenschutzrechtlichen Anforderungen an Normenklarheit kaum entsprechen. Es ist jedoch hervorzuheben, daß die Verwaltungshochschule in Speyer unter Mitwirkung der Staatskanzlei, des ISM und der DSK beispielgebende Regelungen für ihre Einschreibeordnung entwickelt hat, die nach Auffassung der DSK auch von den anderen Hochschulen in angepaßter Weise übernommen werden sollten. Aufgrund der Autonomie der Hochschulen sind die Einwirkungsmöglichkeiten sowohl der DSK wie des Kultusministeriums in diesem Zusammenhang jedoch relativ gering. Kritisch anzumerken bleibt, daß das Kultusministerium seine nach Auffassung der DSK bestehenden Einflußmöglichkeiten hier jedoch nicht genutzt hat.

10.2.2 Örtliche Feststellungen in Hochschulrechenzentren

Örtliche Feststellungen bei einer technischen Hochschule des Landes ergaben, daß – abhängig vom Gegenstand der dort vorrangig betriebenen Wissenschaftsdisziplinen – kaum personenbezogene oder personenbeziehbare Daten verarbeitet werden. Dies gilt jedoch nicht ausnahmslos. So war negativ anzumerken, daß die gesetzlich vorgesehene Verpflichtung zur Regelung des Umgangs mit automatisiert verarbeiteten personenbeziehbaren Daten nicht im vollen Umfang erfüllt worden ist.

Die Datenverarbeitung im Bereich der Studenten- und Bedienstetendaten bot keinen Anlaß zur Beanstandung.

10.3 Archivwesen

Nach nunmehr nahezu zehnjährigen Drängens seitens der DSK und fünf Jahre nach der Vorlage des ersten Entwurfs der Bundesregierung zu einem Bundesarchivgesetz hat auch der rheinland-pfälzische Landtag erste Anstrengungen unternommen, um das aus datenschutzrechtlicher Sicht dringend erforderliche Landesarchivgesetz zu erlassen. Inzwischen liegen Entwürfe sowohl der Landesregierung wie der Fraktionen der SPD und der GRÜNEN vor. Die DSK hat sich bemüht, ihre Vorstellungen bereits im Vorfeld der Beratungen gegenüber dem Kultusministerium zum Tragen zu bringen. Ihre Vorschläge sind dort jedoch kaum berücksichtigt worden. Sie wird weiterhin versuchen, die aus ihrer Sicht wesentlichen datenschutzrechtlichen Gesichtspunkte im Gesetzgebungsverfahren einzubringen. Mit diesem Ziel hat sie an der Anhörung des Kulturpolitischen Ausschusses zum Archivgesetz teilgenommen. Dort hat sie detaillierte Vorschläge unterbreitet, die insbesondere folgende Schwerpunkte betreffen:

– Stärkung des Rechtes der Betroffenen auf Akteneinsicht;

– normenklare Regelung der Nutzungsbefugnisse;

– angemessene Berücksichtigung der Interessen der Nutzungsberechtigten durch angemessene Sperrfristen und angemessenen (reduzierten) Schutz der Interessen betroffener Amtswalter;

– Berücksichtigung der technischen Entwicklung durch eine angemessene Beschränkung der Übernahmemöglichkeiten der Archive für automatisiert gespeicherte personenbezogene Daten. In diesem Zusammenhang hat die DSK die Aufnahme folgender Vorschrift in das Landesarchivgesetz vorgeschlagen:
„Eine Übernahme vollständiger Bestände von in der Verwaltung entstandenem Archivgut darf nur ausnahmsweise erfolgen. Voraussetzung ist, daß der gesamte Datenbestand in besonderer Weise archivwürdig ist."

In welchem Umfang die Vorstellungen der DSK im weiteren Gesetzgebungsverfahren berücksichtigt werden, ist im Zeitpunkt der Erstellung des Tätigkeitsberichts noch nicht absehbar.

11 Wirtschaft und Verkehr

11.1 Datenverarbeitung im Zusammenhang mit dem Fahren und Halten von Kraftfahrzeugen

11.1.1 Das zentrale Verkehrsinformationssystem beim Kraftfahrt-Bundesamt

Die gesetzliche Regelung für das zentrale Kraftfahrzeugregister beim Kraftfahrt-Bundesamt wurde im letzten Tätigkeitsbericht (Tz. 11.1.1) kurz geschildert (§§ 31 – 37 Straßenverkehrsordnung sowie die dazu ergangene Fahrzeugregisterverordnung). Vertreter der Datenschutzbeauftragten des Bundes und der Länder haben zwischenzeitlich ein Prüfkonzept entwickelt, um die gesetzlich vorgeschriebenen Protokollierungen auch in angemessener Weise für Kontrollmaßnahmen zu nutzen. Die DSK wird in der nächsten Zukunft bemüht sein, dieses Prüfkonzept umzusetzen.

11.1.2 Direktabrufverfahren bei örtlichen Halterregistern

Zwischenzeitlich sind nahezu alle örtlichen Kfz-Halterregister automatisiert worden. Damit hat sich die Frage ergeben, unter welchen Voraussetzungen andere öffentliche Stellen diese Halterregister durch Anschlüsse für Direktabrufverfahren nutzen dürfen. Die detaillierten Regelungen im Straßenverkehrsgesetz sowie in der Fahrzeugregisterverordnung haben nicht alle Zweifelsfragen geklärt: So bleibt es fraglich, ob nach dem Zuständigkeitsübergang für die Überwachung des ruhenden Verkehrs auf die Gemeinden (die Ortspolizeibehörden) ein Direktabrufverfahren zwischen den neu entstandenen Verkehrsüberwachungsämtern und den örtlichen Kfz-Zulassungsregistern zulässig ist. Die DSK hat in Abstimmung mit dem ISM die Zulässigkeit entsprechender Online-Verfahren bejaht, obwohl bei strenger wörtlicher Auslegung nur Dienststellen des Polizeivollzugsdienstes der Länder, nicht aber Ortspolizeibehörden anschlußberechtigt sind (§ 12 Abs. 1 Satz 2 Nr. 3 Fahrzeugregisterverordnung). Angesichts der Aufgabenidentität zwischen dem Polizeivollzugsdienst des Landes und den Verkehrsüberwachungsämtern als Teil der Ortspolizeibehörden für den Bereich des ruhenden Verkehrs hat es die DSK aber für vertretbar und angemessen gehalten, hier nach Sinn und Zweck der genannten Vorschrift von einer erweiternden Auslegung auszugehen.

11.1.3 Halterauskünfte durch Kfz-Zulassungsstellen an Private

Die gesetzliche Neuregelung der Kfz-Register hat eine deutliche Beschränkung der Zulässigkeit von Halterauskünften mit sich gebracht: Zur Geltendmachung von Rechtsansprüchen, die nicht mit dem Straßenverkehr im Zusammenhang stehen, sind Halterauskünfte an Privatpersonen nicht mehr möglich (§ 39 StVG). Rechtsanwälte versuchen gelegentlich, diese Regelung zu umgehen. Eine Eingabe hat dies verdeutlicht:

Ein Beschwerdeführer war von einem Rechtsanwalt zur Herausgabe von Fotografien, die er von dem Anwesen eines Privatdetektivs aufgenommen hatte, aufgefordert worden. Für ihn war unverständlich, auf welchem Weg der Rechtsanwalt seine Anschrift erhalten hat. Feststellungen der DSK ergaben, daß der Eigentümer des fotografierten Anwesens das Kennzeichen des Fahrzeugs des Petenten notiert hatte. Diese Information teilte er seinen Rechtsanwälten mit, die bei der zuständigen Kraftfahrzeugzulassungsstelle anfragten, wer Halter des Kraftfahrzeugs sei. Dabei gaben sie auf einem Vordruck an, daß das Fahrzeug des Beschwerdeführers an einem Verkehrsunfall beteiligt gewesen sei.

Die Anforderung der Daten unter Vortäuschung eines unzutreffenden Sachverhalts war unzulässig. Sie hat auch im Ergebnis zu einer rechtswidrigen Datenübermittlung geführt, da eine Auskunft zur Geltendmachung von Herausgabeansprüchen (bez. der Fotografien) nicht hätte erteilt werden dürfen. Der Petent wurde darauf hingewiesen, daß für ihn die Möglichkeit bestand, gem. § 27 LDatG Strafantrag wegen unbefugter Datenbeschaffung zu erstatten.

Die DSK informierte die zuständige Rechtsanwaltskammer und bat um Überprüfung der Angelegenheit aus standesrechtlicher Sicht. Die Kammer hat diesen Fall zum Anlaß genommen, in ihrem Mitteilungsblatt auf die Wahrheitspflicht der Rechtsanwälte hinzuweisen.

Das von dem Petenten eingeleitete Strafverfahren wurde von der zuständigen Staatsanwaltschaft eingestellt, da dem Beschuldigten eine Straftat nicht nachzuweisen sei. Die Einlassung des Rechtsanwalts habe wie folgt gelautet: Nicht er hätte die Abfrage veranlaßt, sondern er hätte den Auftrag einer erfahrenen Büroangestellten erteilt, die aus jetzt nicht mehr nachvollziehbaren Gründen versehentlich den Vordruck für Halteranfragen in Unfallsachen verwendet habe.

Dem Anwalt sei daher, so die Staatsanwaltschaft, nicht nachzuweisen, daß er vorsätzlich vom Gesetz geschützte personenbezogene Daten unbefugt abgerufen oder sich sonstwie verschafft habe.

11.1.4 Zentraldatei der Führerscheinbewerber

Das Innenministerium beabsichtigt, landesweit für alle Führerscheinstellen eine Zentraldatei der Führerscheinbewerber einzurichten. Die hiermit im Zusammenhang stehenden datenschutzrechtlichen Probleme sind vielfältig. Die eingeleitete Abstimmung ist noch nicht abgeschlossen.

11.2 Ermittlungsbefugnisse der Handwerkskammern zum Zweck der Verfolgung von Schwarzarbeit oder Unterbindung unerlaubter Handwerksausübung

Wie in vergangenen Berichtszeiträumen hat die DSK auch in den vergangenen zwei Jahren verschiedene Anfragen erhalten, die die Kompetenz der Handwerkskammern zur Sachverhaltsaufklärung bei Verdacht auf Schwarzarbeit oder des Vorliegens unerlaubter Handwerksausübung betreffen. Unter Berücksichtigung der von ihr in der Vergangenheit dazu entwickelten Auffassung (11. Tätigkeitsbericht, Tz. 11.2; 10. Tätigkeitsbericht, Tz. 8.6 sowie 8.7) hat sie in derartigen Fällen wie folgt argumentiert:
Die Handwerkskammern besitzen im Bereich der Bekämpfung der Schwarzarbeit unter zwei Gesichtspunkten Kompetenzen: Sie können einen Antrag auf Untersagung der Handwerksausübung durch einen Schwarzarbeiter stellen; sie können auch eine Anzeige mit dem Ziel der Verhängung eines Bußgeldes bei der zuständigen Stelle erstatten. Beide Handlungen setzen voraus, daß die Handwerkskammer einer dritten Stelle (der für die Tätigkeitsuntersagung oder der für die Bußgeldverhängung zuständigen Stelle) Informationen übermittelt. Es wäre nicht angemessen, wenn die Handwerkskammer darauf verwiesen würde, den zuständigen Behörden nur Hinweise auf vage Verdachtsfälle zu geben. Ihre gesetzlichen Aufgaben in diesem Zusammenhang (§§ 16 Abs. 3, 91 Abs. 1 Nr. 1 Handwerksordnung) umfassen vielmehr nach Auffassung der DSK auch die Befugnis, entsprechend dem allgemeinen Verwaltungsverfahrensrecht die in Rede stehenden Sachverhalte aufzuklären (insbesondere § 26 Abs. 1 Verwaltungsverfahrensgesetz). Danach bedient sich die Behörde der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere Auskünfte jeder Art einholen.

Im Rahmen des Ermessens, welche Auskünfte eingeholt werden, ist eine Interessenabwägung vorzunehmen. Durch das Einholen von Auskünften bei Dritten wird nämlich diesen grundsätzlich die Tatsache bekannt gemacht, daß Sachverhaltsermittlungen durch die Handwerkskammer durchgeführt werden. Damit könnte für den betroffenen Handwerker eine nachteilige Reaktion seiner Kunden verbunden sein.

Andererseits ist dabei auch zu berücksichtigen, daß jede ermittelnde Behörde zur Aufklärung von Verdachtsfällen die in Betracht kommenden Kunden des Betroffenen befragen müßte. Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz setzt hier sicherlich Grenzen: Das Übermaßverbot ist zu beachten. In den Fällen, die der DSK zur Beurteilung vorgelegt worden sind, war ein Verstoß gegen diesen Rechtsgrundsatz nicht zu konstatieren.

11.3 Datenübermittlungen im Bereich der Gewerbeordnung

11.3.1 Kartei der Gewerbeanmeldungen

Die in den vergangenen Tätigkeitsberichten befürchteten Schwierigkeiten aufgrund fehlender gesetzlicher Regelungen für den Bereich der Kartei der Gewerbeanmeldungen sind im Berichtszeitraum praktisch geworden: Die DSK hatte wiederholt darauf hingewiesen (insbesondere 10. Tätigkeitsbericht, Tz. 8.1.1), daß bei einer automatisierten Führung der Gewerbekartei Datenübermittlungen an private Dritte nicht mehr zulässig seien, wenn die Betroffenen nicht zugestimmt hätten (§ 7 Abs. 1 LDatG).

Nunmehr sind mehrere Städte dazu übergegangen, trotz der geschilderten Problematik die Gewerbekartei zu automatisieren. Die DSK hat, im Interesse einer praktikablen und die Belange der betroffenen Gewerbetreibenden wahrenden Verfahrensweise, folgendes Vorgehen für datenschutzrechtlich zulässig gehalten:

- Bei Neuaufnahmen in das automatisierte Gewerberegister müssen die einzutragenden Gewerbetreibenden die freie Wahl besitzen, ob sie Auskünfte aus dem automatisierten Gewerberegister an private Dritte ausschließen wollen oder nicht. Dies ist durch eine entsprechende Gestaltung der Anmeldeformulare zu gewährleisten.

- Bereits eingetragene Gewerbetreibende sind vor der Umstellung des Verfahrens auf automatisierte Registerführung in geeigneter Weise (durch Veröffentlichungen in der Tagespresse bzw. in Verbandsmitteilungen) darauf hinzuweisen, daß sie das Recht besitzen, entsprechenden Datenübermittlungen zu widersprechen.

Eine solche Verfahrensweise wird dem Wortlaut des Gesetzes (§ 7 Abs. 1 LDatG i.V.m. § 5 LDatG) nicht in vollem Umfang gerecht. Eine andere Lösung wäre aber wohl unangemessen. Die Alternative wäre, daß die Automation in diesem Bereich nicht eingesetzt werden kann. Dies würde ebenfalls gewichtigen Rechtsgütern – wie dem Grundsatz der sparsamen und effektiven Mittelverwendung durch die Verwaltung – widersprechen. Durch die gewählte Verfahrensweise wird zudem in Rechte der Betroffenen nicht eingegriffen.

Es bleibt zu hoffen, daß die zu erwartende Novellierung der Gewerbeordnung auch dieses rechtliche Problem lösen wird.

11.3.2 Ergänzung der Gewerbeordnung um datenschutzrechtliche Vorschriften

In der Vergangenheit hat sich die DSK intensiv bemüht, eine Ergänzung der Gewerbeordnung um datenschutzrechtliche Vorschriften – insbesondere bezüglich der Auskunftserteilung aus dem Gewerberegister – zu erreichen (vgl. 11. Tätigkeitsbericht, Tz. 11.7; 10. Tätigkeitsbericht, Tz. 8.1.1). Nunmehr liegt ein Referentenentwurf aus dem Bundeswirtschaftsministerium zur Änderung datenschutzrechtlich relevanter Vorschriften im Gewerberecht vor. Dieser Entwurf läßt jedoch aus datenschutzrechtlicher Sicht noch mehrere Wünsche offen: In Übereinstimmung mit dem MWV sowie mit dem ISM hat die DSK gefordert, daß Datenübermittlungen aus der Gewerbekartei an private Dritte bereichsspezifisch und ausdrücklich zu regeln sind. Die bislang vorgesehene Verweisung auf Vorschriften der Datenschutzgesetze ist sinnwidrig: Die Regelung des rheinland-pfälzischen Datenschutzgesetzes, die im Zusammenhang mit den automatisierten Gewerberegistern zu unangemessenen Ergebnissen führt, müßte gerade durch besondere Rechtsgrundlagen der Interessenlage im Gewerbebereich angepaßt werden.

Unabhängig davon hat die DSK darauf hingewiesen, daß in der Gewerbeordnung zusätzliche und normenklare Rechtsgrundlagen für Datenerhebungen und Datenübermittlungen durch Gewerbebehörden aufgenommen werden müßten. Die bisher vorliegenden Formulierungen sind zum Teil noch zu unklar und unbestimmt. So sollten insbesondere die Voraussetzungen von Sperrung und Löschung der bei den Gewerbebehörden gespeicherten Daten präziser geregelt werden.

Das Gesetzgebungsverfahren sollte aus Sicht der DSK zügig vorangetrieben werden. Auch darauf hat sie das Wirtschaftsministerium hingewiesen.

11.4 Ernährungsvorsorgegesetz, Ernährungssicherstellungsgesetz

Zur Bewältigung von Notsituationen, in denen zwar die Sicherheit des Landes nicht militärisch bedroht ist, in denen aber die Versorgung der Bevölkerung in wesentlichen Teilen des Bundesgebietes ernsthaft gefährdet ist, hat der Bund eine eigenständige Rechtsgrundlage in Form eines Ernährungsvorsorgegesetzes geschaffen.

Gleichzeitig wurde das Ernährungssicherstellungsgesetz, das sich primär auf den Verteidigungsfall bezieht, entsprechend geändert.

Datenschutzrechtliche Fragen haben sich insofern gestellt, als insbesondere zur Durchführung des Ernährungsvorsorgegesetzes Auskunftspflichten der Bürger eingeführt werden mußten. Die DSK hat zunächst angeregt, die dahin zielende Verordnungsermächtigung zu konkretisieren.

Unabhängig von dieser zentralen Frage hat sie weiter darauf hingewiesen, daß aus ihrer Sicht die Zweckbindung der erhobenen Daten klarer und eindeutiger zu formulieren ist. Außerdem hat sie vorgeschlagen, auch in das Ernährungssicherstellungsgesetz ein entsprechendes Verwertungsverbot einzufügen. Der Bundesgesetzgeber ist den zuletzt genannten Anregungen nachgekommen.

11.5 Verwertung von Informationen der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) durch Sparkassen

Die DSK hat in ihrem 10. Tätigkeitsbericht (Tz. 8.3) anläßlich der Neufassung der allgemeinen Geschäftsbedingungen für Banken und Sparkassen das Bankauskunftsverfahren und auch das Verhältnis zwischen Banken und Schufa dargestellt. In Eingaben ist die nach wie vor bestehende Problematik des Schufa-Auskunftsverfahrens deutlich geworden. Beispielsweise hat ein Beschwerdeführer folgenden Fall vorgetragen:
Er sei überschuldet und habe dementsprechend negative Eintragungen bei der Schufa. Um als Selbständiger (im Rahmen eines medizinischen Berufs) tätig sein zu können, sei er dennoch auf ein Girokonto angewiesen. Dieses Konto war von einer Sparkasse auch eingerichtet worden. Aufgrund einer negativen Schufa-Auskunft löste die Sparkasse das Konto, das stets nur Guthaben aufwies, jedoch einseitig auf.

Der Beschwerdeführer trug vor, daß ohne Girokonto eine Teilnahme am Geschäftsverkehr unmöglich sei und daß ihm auch die Begleichung von Schulden nicht gelingen werde, wenn er keine Einnahmen erzielen könne.

Die DSK hat die damit zusammenhängenden Fragen der zulässigen Verwertung von Schufa-Daten mit dem Sparkassen- und Giroverband Rheinland-Pfalz erörtert.

Sie hat im Ergebnis folgende Auffassung vertreten:

- Wenn ein Sparkassenkunde bereits bei der Eröffnung eines Girokontos zu erkennen gibt, daß er ausschließlich ein Konto auf Guthabenbasis führen will, also weder Überziehungskredite noch die Ausstellung von Euro-Scheckkarten etc. beantragt werden, ist das Verlangen in eine Einwilligung zur Auskunftseinholung bei der Schufa nicht gerechtfertigt.

- Falls dennoch eine entsprechende Einwilligung eingeholt wird oder falls ohne Einwilligung Schufa-Abfragen erfolgen, sind die daraus erlangten Informationen grundsätzlich nicht verwertbar, sofern der Betroffene keine rechtswidrigen schädigenden Handlungen gegenüber einem Kreditinstitut begangen hat.

Für die DSK war und ist nicht ersichtlich, welche Gründe bei einer Kontoführung auf Guthabenbasis in der geschilderten Form für ein Kreditinstitut bestehen könnten, das Kontoverhältnis zu kündigen, wenn bislang dieses Institut durch das Verhalten des Konteninhabers nicht geschädigt wurde. Nur im letztgenannten Fall wäre ein berechtigtes Interesse an einer Auflösung des auf Guthabenbasis geführten Girokontoverhältnisses denkbar.

Die DSK hält es inbesondere aufgrund der besonderen Gemeinwohlverpflichtung der Sparkassen sowie aufgrund der Bedeutung des bargeldlosen Zahlungsverkehrs im Geschäftsleben für verfassungsrechtlich geboten, nach diesen Grundsätzen zu verfahren.

In diesem Sinne hat sie gegenüber dem Sparkassen- und Giroverband Rheinland-Pfalz Stellung genommen und diesen gebeten, entsprechende konkretisierende Empfehlungen an seine Mitgliedssparkassen zu geben.

12 Sozialleistungsbereich

12.1 Gesundheitsreformgesetz

Unter dem Druck der Kostenentwicklung im Gesundheitswesen wurde die Strukturreform im Jahre 1988 zielstrebig vorangetrieben und abgeschlossen. Das vom Deutschen Bundestag am 25. November 1988 verabschiedete Gesundheitsreformgesetz ersetzt die Vorschriften des Zweiten Buchs der Reichsversicherungsordnung über die gesetzliche Krankenversicherung und wurde als Fünftes Buch in das Sozialgesetzbuch eingefügt.

Die Dringlichkeit des gesetzgeberischen Handlungsbedarfs war angesichts der immensen Kosten des Gesundheitswesens und der ständig steigenden Beitragssätze der Krankenversicherung nicht zu bestreiten. Ebenso unbestreitbar war aber auch die datenschutzrechtliche und datenschutzpolitische Relevanz der gesetzlichen Neuordnung. Diese lag einerseits in der Tatsache begründet, daß die gesetzliche Krankenversicherung im Grundsatz als Pflichtversicherung organisiert ist. Hieraus folgt, daß die Betroffenen auf die Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten keinen oder nur einen sehr begrenzten Einfluß haben. Andererseits zielt das Gesetz auf Kostendämpfung. Seine Instrumente zur Erreichung dieses Ziels sind die Verbesserung der Transparenz des Leistungsgeschehens, die Schaffung der Voraussetzungen für die Prüfung der Wirtschaftlichkeit, der Zweckmäßigkeit und Notwendigkeit abgerechneter Leistungen und die Bekämpfung von Abrechnungsmanipulationen. Dies läßt sich nur dadurch erreichen, daß Leistungs- und Gesundheitsdaten in stärkerem Umfange als in der Vergangenheit erfaßt und in automatisierten Verfahren verarbeitet, insbesondere übermittelt werden.

Aus der Sicht des Datenschutzes war zu fordern, daß der Umfang der Datenerfassung und -verarbeitung auf das unabdingbare Maß beschränkt und präzise und für die Betroffenen nachvollziehbar im Gesetz festgelegt wird.

Es ist anzuerkennen, daß sich das federführende Bundesministerium für Arbeit und Sozialordnung bei der Ausarbeitung des Gesetzentwurfs gegenüber den von der Datenschutzseite vorgetragenen Anliegen aufgeschlossen zeigte. Es gelang, schon im Verfahren der Ausarbeitung des Regierungsentwurfs eine ganze Reihe von Forderungen des Datenschutzes, die in den Vorentwürfen zunächst nicht berücksichtigt waren, durchzusetzen. So ist beispielsweise die Speicherung aller erbrachten und verordneten Leistungen in einem sog. „Versichertenkonto" entfallen. Ein weiteres Beispiel ist die Bestimmung konkreter Löschungsfristen für Daten über Leistungsvoraussetzungen.

Weitere Erfolge beruhen auf den Empfehlungen der Datenschutzbeauftragten in ihrem Beschluß vom 6. Juni 1988.

Trotz des Bemühens um präzise Regelungen stellen sich immer noch Auslegungsfragen. So ist beispielsweise unklar, ob Diagnoseangaben auf Krankenscheinen zur kassenärztlichen Abrechnung aufgrund der nach dem Gesundheitsreformgesetz geänderten Rechtslage noch zulässig sind. Eine ausdrückliche Rechtsgrundlage hierfür ist dem Gesetz jedenfalls nicht zu entnehmen. Eine weitere Auslegungsfrage, die gegenwärtig in der Diskussion ist, betrifft die Durchführung von Qualitätsprüfungen durch die Kassenärztlichen Vereinigungen. Es ist unklar, ob diese für Prüfungszwecke von den behandelnden Ärzten Patientenunterlagen wie Karteikarten, EKG-Streifen, Arztbriefe und Befunddokumentationen anfordern dürfen. Das Gesetz enthält, anders als bei der Durchführung von Wirtschaftlichkeitsprüfungen, keine Befugnisnorm für die Datenübermittlung für Zwecke der Qualitätsprüfung. Der Bundesbeauftragte für den Datenschutz ist um Klärung dieser und anderer Auslegungsfragen bemüht.

12.2 Einladung zu Krebsfrüherkennungsuntersuchungen

Um die Auslegung von Vorschriften des Sozialgesetzbuchs – V. Buch – (SGB V) ging es auch bei einer Anfrage, die das MUG an die DSK richtete. Mehrere gesetzliche Krankenversicherungen beabsichtigten, ein Projekt durchzuführen, das auf eine Verbesserung der Akzeptanz von Krebs-Früherkennungsuntersuchungen zielte. Die gesundheitspolitische Bedeutung solcher Maßnahmen steht angesichts einer Beteiligung von nur rund 32 % der Frauen und 11 % der Männer an Früherkennungsuntersuchungen außer Frage.

Die Krankenkassen beabsichtigten, ihre Versicherten, die an Untersuchungen zur Früherkennung von Krebserkrankungen nicht teilnehmen, zu erfassen und in persönlichen Anschreiben (Einladung) auf das Leistungsangebot (jährlich eine Untersuchung für Frauen ab dem 20., für Männer ab dem 45. Lebensjahr) hinzuweisen.

§ 284 Abs. 1 Nr. 4 SGB V läßt zu, daß Krankenkassen personenbezogene und personenbeziehbare Daten für Zwecke der Krankenversicherung erheben und erfassen, soweit diese für die Gewährung von Leistungen an Versicherte einschließlich der Verfahren bei Kostenerstattung und in Härtefällen erforderlich sind. Als Leistungsart nennt § 11 u. a. die Verhütung und Früherkennung von Krankheiten.

Die Vorschriften über die Leistungen zur Früherkennung von Krankheiten (§§ 25 und 26 SGB V) regeln die Anspruchsvoraussetzungen für Früherkennungsuntersuchungen. Die Durchführung eines Einladungsverfahrens für solche Untersuchungen ist danach als Aufgabe der Krankenkasse nicht vorgesehen.

Hinweise auf Früherkennungsuntersuchungen sind jedoch als Maßnahmen der Gesundheitsförderung und Krankheitsverhütung i. S. des § 20 SGB V anzusehen. Nach dieser Vorschrift haben die Krankenkassen ihre Versicherten allgemein über Gesundheitsgefährdungen und über die Verhütung von Krankheiten aufzuklären. Die Verwendung des Begriffs „allgemein" bringt nach Auffassung der DSK zum Ausdruck, daß Aufklärungsmaßnahmen weder als Pflichtleistungen noch als Ermessensleistungen zugelassen sind, wenn diese die Erhebung und Aufzeichnung von Daten über das Verhalten des Versicherten zur Voraussetzung haben. Es besteht also keine Befugnis, Verhaltensdaten oder sonstige Informationen zu dem Zweck zu erheben und zu verarbeiten, die Versicherten zur Inanspruchnahme von Leistungen der Gesundheitsförderung oder Krankheitsverhütung aufzufordern. Eine Datenerfassung für diesen Zweck widerspräche demzufolge § 284 Abs. 1 Nr. 4 SGB V.

Um Mißverständnisse auszuschließen: Die Krankenkassen sind nach der Rechtslage nicht gehindert, regelmäßig alle Versicherten anzuschreiben und zur Teilnahme an Früherkennungsuntersuchungen einzuladen. Sie müssen aber in Kauf nehmen, daß die Einladung auch solche Versicherte erreicht, die an solchen Gesundheitsuntersuchungen bereits teilgenommen haben.

Es bestehen auch keine datenschutzrechtlichen Bedenken gegen eine Lösung, wie sie im konkreten Falle schließlich gefunden wurde: Alle Versicherten werden angeschrieben, über die gesetzlichen Leistungen zur Früherkennung von Krankheiten aufgeklärt und gebeten, ihre schriftliche Zustimmung zur regelmäßigen Einladung zu erteilen. In der Folge ergeht eine Einladung nur noch an die Versicherten, die diesem Verfahren zugestimmt haben.

Auch wenn die gesundheitspolitische Zielsetzung eines Einladungsverfahrens in besonderem Maße förderungswürdig ist und eine Behinderung durch den Datenschutz vielleicht wenig Verständnis findet, so darf doch nicht übersehen werden, daß es hier um eine allgemein bedeutsame Frage und um sensible Daten geht. Schon gibt es eine Krankenkasse, die zugelassene Ärzte aufforderte ihr mitzuteilen, welche Patienten übergewichtig sind, damit – ebenfalls auf der Grundlage des § 20 SGB V – gezielte Maßnahmen der Ernährungsberatung eingeleitet werden können. Es fällt sicherlich nicht schwer sich vorzustellen, daß sich Gesundheitsförderungsmaßnahmen dieser Art beliebig ausdehnen lassen. Denkbar sind Einladungen an Raucher zur Teilnahme an Entwöhnungsbehandlungen, an Alkohol- oder sonstige Suchtkranke. Der Gesetzgeber hat die mit solchen gezielten Maßnahmen verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht nicht zugelassen. Es ist allein Sache des Arztes, dem sich der Patient im Vertrauen auf dessen Verschwiegenheitspflicht offenbart hat, notwendige Behandlungsmaßnahmen einzuleiten und durchzuführen.

12.3 Kassenübergreifende Wahrnehmung von Prüfungsaufgaben nach § 106 SGB V

Mit dem Ziel, die Wirtschaftlichkeit der Aufgabenwahrnehmung zu erhöhen, haben sich Krankenkassen in verschiedenen Landesteilen in Verbänden zusammengeschlossen. Rechtsgrundlage hierfür ist § 219 SGB V (früher § 406 RVO).

Die DSK wurde von einem solchen Verband um Stellungnahme zu der Frage ersucht, ob es zulässig ist, die den Kassen nach § 106 SGB V obliegenden Überwachungsaufgaben – Wirtschaftlichkeitsprüfung der Kassenärztlichen Versorgung – in der Weise wahrzunehmen, daß die hierfür erforderlichen Daten aller angeschlossenen Kassen von dem Verband in eine Datenbank übernommen und kassenübergreifend ausgewertet werden.

Ohne Zweifel ermöglicht gerade diese kassenübergreifende Auswertung von Daten eine besonders effektive Aufgabenwahrnehmung. Zugleich stellt sich aber auch ein datenschutzrechtliches Problem, denn einer kassenübergreifenden Auswertung geht, datenschutzrechtlich betrachtet, zwangsläufig eine regelmäßige Datenübermittlung zwischen den beteiligten Kassen voraus, auch wenn diese Übermittlung nur innerhalb der gemeinsamen Prüfstelle erfolgt. In der Datennutzung für Zwecke der jeweils anderen Kasse ist ein Übermittlungsvorgang enthalten.

Die DSK vertritt die Auffassung, daß der Gesetzgeber eine kassenübergreifende Erfüllung der Aufgaben nach § 106 SGB V nicht im Blick hatte, denn sonst hätte er, der Gesetzessystematik folgend, spezielle Übermittlungsregelungen geschaffen.

Im Bezug auf den konkreten Fall bedeutet dies, daß es der einzelnen angeschlossenen Kasse von Gesetzes wegen – aufgrund fehlender Übermittlungsregelungen – und wegen der sachlichen Begrenzung ihres Wirkungsbereichs – weil sie über die Überprüfungsdaten anderer Kassen nicht verfügt – nicht möglich ist, die Aufgaben nach § 106 SGB V kassenübergreifend wahrzunehmen. Folglich ist auch der Kassenverband hieran gehindert.

Es ist im übrigen zu berücksichtigen, daß die kassenübergreifende Prüfung der Wirtschaftlichkeit nicht etwa deshalb unterbleibt, weil der Verband an der Aufgabenwahrnehmung gehindert ist. Sie ist vielmehr nach den gesetzlichen Vorschriften von den Kassenärztlichen Vereinigungen, die über eine wesentlich größere Datenbasis verfügen als die einzelnen Krankenkassen, vorzunehmen.

Das SFM als oberste Aufsichtsbehörde bestätigte zwar, daß eine ausdrückliche gesetzliche Grundlage für die Aufgabenwahrnehmung in der vorgesehenen Weise nicht vorhanden ist, vertrat aber entgegen der DSK die Auffassung, daß eine Befugnis aus § 219 Satz 2 SGB V i. V. m. § 94 Abs. 4 und § 88 Abs. 1 Satz 1 SGB X hergeleitet werden könne. Die DSK erklärte, daß ihre rechtlichen Bedenken gegen die kassenübergreifende Aufgabenwahrnehmung hierdurch nicht ausgeräumt seien, denn auch den zitierten Bestimmungen kann eine rechtliche Grundlage für die mit dieser Aufgabenwahrnehmung verbundene Datenübermittlung nicht entnommen werden.

12.4 Sozialdatenschutz im Krankenversicherungsbereich

Zu den Bereichen der öffentlichen Verwaltung mit besonderer Datenschutztradition gehören die Krankenkassen, die Krankenkassenverbände und die Kassenärztlichen Vereinigungen. Im Schriftwechsel mit der DSK und in Gesprächen wird dies von den Geschäftsleitungen dieser Einrichtungen immer wieder betont.

Sicherlich kann im Grundsatz davon ausgegangen werden, daß sich die Bediensteten ihrer besonderen Verschwiegenheitspflichten bewußt sind, auch wenn die dienstrechtliche Geheimhaltungsverpflichtung schon vor vielen Jahren erfolgte. Es ist im übrigen Aufgabe der nach § 79 SGB X i. V. m. §§ 28, 29 BDSG zu bestellenden Datenschutzbeauftragten der Sozialleistungsträger, die bei der Verwaltung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den gesetzlichen Vorschriften zum Schutze der Sozialdaten vertraut zu machen und die danach bestehenden Verpflichtungen bei Schulungsmaßnahmen gelegentlich in Erinnerung zu rufen. Der DSK ist bekannt, daß einzelne Sozialleistungsträger – wie z. B. die Kassenärztlichen Vereinigungen – der Schulung von Mitarbeitern in Datenschutzfragen eine große Bedeutung beimessen.

Bisweilen klafft indessen zwischen dem hohen Anspruch von Leistungsträgern bezüglich der Sensibilität für Datenschutzfragen und der Realität eine deutliche Lücke, die auch bei Berücksichtigung einer gewissen Abstumpfung durch die Routine der täglichen Arbeit nicht zu entschuldigen ist.

Zu den kritikwürdigen Vorgängen zählt beispielsweise das Verhalten eines Krankenkassenverbandes. Eine Bezirksregierung, die in einem Ordnungswidrigkeitsverfahren wegen Verstoßes gegen die Vorschriften der Apothekenbetriebsverordnung ermittelte, wollte von diesem Verband wissen, wie viele Rezepte von einem bestimmten Arzt ausgestellt worden waren. Gefragt war also nur nach der Zahl der Rezepte. Der Verband hingegen übersandte der Bezirksregierung kurzerhand die von diesem Arzt ausgestellten Rezepte und offenbarte auf diese Weise Diagnosen und andere empfindliche Informationen, die durch das Sozialgeheimnis geschützt sind.

In einem anderen Falle teilte der Geschäftsführer einer Ortskrankenkasse dem Arbeitgeber eines ehemaligen Kassenmitglieds mit, welche Begründung von diesem für den Übertritt zu einer Ersatzkasse gegeben worden war.

Die Offenbarung von Sozialdaten erfolgte in diesem Falle, ebenso wie die Rezeptweitergabe unter Verstoß gegen die Vorschriften zum Schutze des Sozialgeheimnisses und wurde von der DSK beanstandet.

Eine andere Krankenkasse wiederum vervielfältigte einen Brief mit den anonymisierten Anamnesedaten dialysepflichtiger Patienten und verschickte die Kopien an niedergelassene Ärzte. Sie bezweckte mit dieser Maßnahme, die Ärzte davon zu überzeugen, daß nach Ansicht eines renomierten Spezialisten auf dem Gebiet der Dialyseversorgung keine Bedenken bestünden, eine neugeschaffene ortsansässige Dialysestation zu nutzen. Die DSK hatte zwar keine Möglichkeit aufzuklären, ob, wie in einer Eingabe behauptet, die Anamnesen für die Empfänger der Briefe tatsächlich personenbeziehbar waren. Sie wies aber die Verantwortlichen darauf hin, daß es auch zu ihren dienstlichen Pflichten gehört, jeden Anschein zu vermeiden, als wären sie sich der besonderen Verpflichtung zur Geheimhaltung amtlicher Vorgänge nicht bewußt. Öffentlich Bedienstete haben das Vertrauen zu rechtfertigen, das in ihre Amtsführung gesetzt wird. Dies gilt insbesondere für die Mitarbeiter einer Krankenversicherung, die von Berufs wegen Zugang zu außerordentlich sensiblen Informationen haben.

Ein letztes Beispiel:
Dem inzwischen in den Ruhestand versetzten Geschäftsführer einer Allgemeinen Ortskrankenkasse wird zur Last gelegt, an eine Hörgeräteakustikfirma mehr als 200 Anschriften von versicherten Hörgeräteträgern unbefugt überlassen zu haben. Die Staatsanwaltschaft ermittelt wegen Bestechlichkeit.

12.5 Rentenreformgesetz 1992

Nach Abschluß der Gesundheitsreform zielten weitere Reformbestrebungen auf eine Anpassung der Rentenversicherung an die veränderten tatsächlichen und rechtlichen Verhältnisse. Der Entwurf eines Rentenreformgesetzes wurde im März dieses Jahres von den Fraktionen der CDU/CSU, SPD und F.D.P. im Bundestag eingebracht, am 9. November 1989 von Deutschen Bundestag in dritter Lesung und am 1. Dezember 1989 vom Bundesrat verabschiedet.

Im Mittelpunkt steht die Konsolidierung der Rentenfinanzierung und die Weiterentwicklung wichtiger Strukturelemente der Rentenversicherung. Das gegenwärtig noch in sechs Gesetzen enthaltene Rentenversicherungsrecht soll im 6. Buch des Sozialgesetzbuchs zusammengefaßt und auch für den Nichtfachmann verständlich und durchsichtig gestaltet werden.

Wie im Krankenversicherungsrecht haben die Reformbestrebungen auch in der Rentenversicherung eine starke datenschutzrechtliche Relevanz. Dies ist verständlich angesichts der Tatsache, daß die Grundzüge des heute noch geltenden Rentenrechts vor rund 80 Jahren in der Reichsversicherungsordnung kodifiziert wurden. Es fehlen normenklare Regelungen über Befugnisse zur Erhebung, Speicherung, Löschung, Auswertung und Weitergabe personenbezogener Daten.

Nach heutigem Rechtsverständnis setzt der Zwang zur Angabe personenbezogener Daten im Rahmen des Versicherungsverhältnisses voraus, daß der Gesetzgeber Art und Umfang der erforderlichen Daten präzise bestimmt, die Verwendungszwecke festlegt und damit die rechtlichen Grundlagen für Eingriffe in das informationelle Selbstbestimmungsrecht schafft.

Die Datenschutzbeauftragten des Bundes und der Länder sowie die DSK haben in der Konferenz am 5./6. April 1989 eine Entschließung verabschiedet. Die Forderungen dieser Entschließung wurden teilweise bei der Gesetzesarbeit berücksichtigt. Aufgrund der Veränderung des Entwurfs als Folge der Ausschußberatungen entstand jedoch ein neues Datenschutzproblem:

Das Gesetz erlaubt den automatisierten Direktabruf aller Rentendaten nicht nur durch die Rentenversicherungsträger, sondern auch durch die gesetzliche Krankenversicherung, die Bundesanstalt für Arbeit und die Deutsche Bundespost, soweit sie mit der Berechnung und Auszahlung von Sozialleistungen betraut ist. Darüber hinaus soll der Direktabruf auch den entsprechenden ausländischen Stellen ermöglicht werden.

Eine so umfassende Erlaubnis zum Direktabruf geht erheblich über die Informationsbedürfnisse der genannten Leistungsträger hinaus. Sie birgt für die Versicherten große Risiken, weil die Datenflüsse in diesem Abrufverfahren weder begrenzbar noch kontrollierbar sind. Dies gilt in noch stärkerem Maße für den Datenabruf aus dem Ausland, der ebenfalls durch das Gesetz zugelassen ist.

Leider ist es nicht mehr gelungen, über das Zustimmungsverfahren des Bundesrates eine Änderung zu erreichen.

12.6 Benachrichtigung von Sozialämtern und Ausgleichsämtern über Rentenanträge

Die Weiterentwicklung des Datenschutzrechts zwingt die Sozialleistungsträger, Informationsvorgänge immer wieder daraufhin zu überprüfen, ob sie den gewandelten rechtlichen Anforderungen an den Sozialdatenschutz noch entsprechen. Leicht wird übersehen, daß eine „aus alter Gewohnheit" beibehaltene regelmäßige Informationsweitergabe an andere Behörden vor dem Hintergrund der am Verhältnismäßigkeitsprinzip zu messenden strikten Offenbarungsenumeration in den §§ 67 ff. SGB X nicht mehr zulässig ist.

So verhielt es sich auch mit der Unterrichtung von Sozialämtern und Ausgleichsämtern über eingegangene Rentenanträge durch die Versicherungsämter mehrerer größerer Städte. Auf den ersten Blick erschien die Zweckbestimmung dieser Unterrichtung einleuchtend, denn die Übermittlungsempfänger sollten in die Lage versetzt werden, eventuell bestehende Ersatzansprüche unmittelbar beim Versicherungsträger anzumelden. Die datenschutzrechtliche Kehrseite ist freilich ebenfalls leicht erkennbar: Die Datenübermittlung ist in der großen Zahl der Fälle nicht erforderlich, in denen der Rentenantragsteller keine anderen Sozialleistungen oder Leistungen nach dem Lastenausgleichsgesetz bezieht bzw. beantragt oder wenn er solche Leistungen zwar bezieht, seinen gegenüber dem Leistungsträger bestehenden Auskunftspflichten aber nachgekommen ist. Es ist ferner zu berücksichtigen, daß Rentenanträge nach § 16 Abs. 1 Satz 1 SGB I in erster Linie beim zuständigen Leistungsträger gestellt werden, so daß die Versicherungsämter keineswegs in allen Fällen von Rentenanträgen Kenntnis erlangen.

Die Auffassung der DSK, daß eine generelle Offenbarungsbefugnis der Versicherungsämter nicht besteht, wurde vom SFM geteilt. Die Versicherungsämter wurden entsprechend unterrichtet.

Die Erörterungen mit dem FM und mit der Arbeitsgemeinschaft der Sozialversicherungsträger ergaben, daß unberechtigte Leistungsgewährungen oder Einnahmeausfälle aufgrund der unterbleibenden Benachrichtigung über die Rentenantragstellung nicht zu befürchten sind.

12.7 Gesetz zur Einführung eines Sozialversicherungsausweises

Das Instrumentarium zur Bekämpfung sozialschädlichen Verhaltens wurde nicht nur durch das Gesundheitsreformgesetz weiterentwickelt. Mit der Einführung eines Sozialversicherungsausweises realisierte der Gesetzgeber eine Konzeption, die schon seit vielen Jahren in der Diskussion ist. Das Ziel ist die Eindämmung von Schwarzarbeit, der illegalen Beschäftigung, des Mißbrauchs von Sozialleistungen und der mißbräuchlichen Ausnutzung der Geringfügigkeitsgrenzen.

Der durch Gesetz vom 6. Oktober 1989 eingeführte fälschungssichere Ausweis ist bei der Beschäftigungsaufnahme vorzulegen und es besteht eine Mitführungspflicht, wenn eine unmittelbare Überprüfung des Beschäftigungsverhältnisses innerhalb von Lohn- und Meldeunterlagen auf der Arbeitsstätte nicht möglich ist (z. B. Bau-, Schausteller-, Gebäudereinigungsgewerbe). Der Ausweis enthält die Versicherungsnummer der Rentenversicherung, den Namen des Beschäftigten und, in Fällen, in denen eine Mitführungspflicht besteht, sein Lichtbild.

Behörden und Stellen, die Sozialleistungen gewähren (beispielsweise Sozialämter, Arbeitsämter oder Krankenkassen) können verlangen, daß der Hilfeempfänger bei ihnen seinen Ausweis hinterlegt. Kommt er diesem Verlangen nicht nach, können die Leistungen ganz oder teilweise versagt werden. Das gleiche Recht hat ein Arbeitgeber, solange er dem Beschäftigten den Lohn oder das Gehalt wegen Arbeitsunfähigkeit weiter bezahlt. Es besteht ferner eine Meldepflicht des Arbeitgebers für solche Beschäftigten, die bei Beschäftigungsbeginn keinen Ausweis vorlegen können. In Fällen der Mitführungspflicht hat der Arbeitgeber bei der Beschäftigungsaufnahme eine Sofortmeldung zu erstatten.

Die Krankenkassen können von den Beschäftigten Auskünfte über die Hinterlegung des Sozialversicherungsausweises verlangen. Erforderlichenfalls können sie andere Sozialleistungsträger darüber unterrichten, daß der Ausweis nicht vorgelegen hat und ihnen weitere für den Leistungsbezug wichtige Informationen geben.
Es entsteht ferner eine Zentraldatei der geringfügig Beschäftigten bei der Datenstelle der Rentenversicherungsträger (VDR).

Die datenschutzrechtliche Bewertung des Gesetzes führt auch hier in den Zwiespalt zwischen der Anerkennung der Notwendigkeit, ein unbestreitbar wichtiges gesellschaftspolitisches Problem zu lösen, und der Erkenntnis, daß damit gewichtige Eingriffe in das informationelle Selbstbestimmungsrecht verbunden sind. Es ist unvermeidbar, daß von den Überwachungs–

und Kontrollmaßnahmen ganz überwiegend solche Bürger betroffen sein werden, die weder einer Schwarzarbeit nachgehen, noch in anderer Weise Anlaß zu derartigen Maßnahmen geben. Die Rentenversicherungsnummer auf dem Sozialversicherungsausweis ist im Grundsatz – auch wenn der Gesetzgeber dies nicht zuläßt – zur Erschließung anderer Dateien gut geeignet. Ihre Streuung durch die vielfältige Verwendung des Sozialversicherungsausweises birgt die Gefahren, die schon Mitte der siebziger Jahre, also in der Anfangszeit des Datenschutzes, zur Ablehnung eines allgemeinen Personenkennzeichens führten.

Wie sehr die Auffassungen über die datenschutzrechtlichen Bewertungen des Versicherungsausweises differieren, erhellt die Tatsache, daß sich die Datenschutzbeauftragten nicht auf eine gemeinsame Beurteilung verständigen konnten. Festzustellen bleibt jedenfalls, daß ein weiteres Mal die durch die automatisierte Datenverarbeitung eröffneten Möglichkeiten zu mehr Kontrolle und Überwachung des Bürgers genutzt werden.

12.8 Datenschutz bei der Sozialhilfegewährung

12.8.1 Allgemeines

Ein deutlicher zahlenmäßiger Anstieg war im Berichtszeitraum bei solchen Eingaben zu verzeichnen, die den Bereich der Sozialhilfegewährung betreffen. Die ihnen zugrunde liegenden Konfliktsituationen entsprachen fast ausnahmslos dem gleichen Muster: Die Prüfung des Bestehens einer Leistungspflicht oder ihres Umfanges veranlaßt die Behörden zur Erhebung oder Übermittlung von Informationen über die persönlichen Lebensumstände des Betroffenen, dessen Interesse wiederum darauf gerichtet ist, diese Informationen zurückzuhalten. Hierfür kann es verschiedene Gründe geben. Ein wichtiger Grund ist die natürliche Scheu des Betroffenen, die Tatsache seiner Bedürftigkeit außerhalb des unmittelbar für die Sachbearbeitung zuständigen Kreises von Behördenbediensteten bekanntwerden zu lassen. Dies lag sicherlich im Blickfeld des Gesetzgebers, der die Informationsverarbeitung im Sozialleistungsbereich unter den besonderen Schutz des Sozialgeheimnisses stellte (§ 35 SGB I)

12.8.2 Beauftragung von Unternehmen durch Sozialämter

Durch eine Eingabe erhielt die DSK den Hinweis auf die Praxis einzelner Sozialämter, in Fällen, in denen die Reparatur von Haushaltsgeräten beantragt wurde, ohne die Zustimmung des Hilfeempfängers und ohne die Erteilung eines Kostenübernahmebescheids Handwerksbetriebe unmittelbar zu veranlassen, die Arbeiten auszuführen und die Reparaturkosten unmittelbar, also unter Umgehung des Sozialhilfeempfängers abzurechnen. Hiermit ist zwangsläufig eine Offenbarung der Tatsache des Sozialleistungsbezugs verbunden.

Das MSI vertrat in seiner Stellungnahme hierzu die Auffassung, daß es im Regelfalle zur sach- und preisgerechten Ausführung von Reparaturen an Haushaltsgeräten von Sozialhilfeempfängern nicht notwendig ist, daß die Sozialhilfebehörde selbst einen Handwerksbetrieb beauftragt und bezahlt. Eine ausreichende Kontrolle lasse sich auch dadurch gewährleisten, daß der Sozialhilfeempfänger einen Kostenvoranschlag zur Prüfung vorlege, mit einer Barbeihilfe die Reparatur dann bezahle und später wiederum die Rechnung zur Einsichtnahme vorlege.

Eine direkte Durchführung der Reparatur auf Veranlassung der Sozialhilfebehörde könnte – von Fällen des ausdrücklichen Einverständnisses abgesehen – nur in Einzelfällen in Betracht kommen, in denen aufgrund der besonderen persönlichen Verhältnisse des Sozialhilfeempfängers die Gefahr bestehe, daß dieser einen zu Reparaturzwecken ausgezahlten Barbetrag nicht ordnungsgemäß verwende.

Bereits vor längerer Zeit wurde bekannt, daß Sozialhilfebehörden dazu übergingen, Sozialhilfeempfängern an Stelle von Bargeldleistungen für Bekleidung oder auch Einrichtungsgegenstände Hilfe in der Weise zu gewähren, daß sie Waren vom Versandhandel liefern lassen. Der Sachverhalt war Gegenstand einer Kleinen Anfrage im Landtag.

In der Antwort auf diese Kleine Anfrage – Drucksache 11/327 – bestätigte das Ministerium für Soziales und Familie, daß einige Träger der Sozialhilfe schon jahrelang vor allem Elektrogeräte wie Kühlschränke und Waschmaschinen über örtliche Filialen eines Versandhauses beziehen und an Hilfesuchende weitergeben. Die datenschutzrechtliche Beurteilung des Vorganges deckt sich mit der Rechtsauffassung der DSK:

- Grundsätzlich ist die Deckung eines einmaligen Bedarfs aus dem Leistungsangebot des Versandhandels rechtsaufsichtlich nicht zu beanstanden, wenn der Hilfeempfänger zustimmt.

- Dem Hilfeempfänger wird ein Preisvergleich und eine daraus evtl. resultierende Entscheidung für eine Barleistung nur im Ausnahmefall vorenthalten, wenn z. B. aufgrund der persönlichen Umstände (unwirtschaftliches Verhalten o. ä.) eine zweckentsprechende Verwendung fraglich ist.

– Datenschutzrechtliche Belange sind nicht berührt, wenn sich der Träger der Sozialhilfe bei einer Sachleistung die Waren liefern läßt und sie selbst an den Hilfeempfänger weitergibt. Dem Lieferanten werden Daten des Hilfeempfängers nicht bekannt. Will der Träger der Sozialhilfe dagegen eine Warenbestellung, die zur unmittelbaren Auslieferung durch das Versandhaus an den Hilfeempfänger führt, vornehmen, ist dies nach § 35 SGB I i. V. m. §§ 67 ff SGB X nur mit ausdrücklicher Zustimmung des Hilfeempfängers möglich.

12.8.3 Verweisung von Antragstellern auf Sozialhilfe an freie Träger

Von manchen Sozialämtern werden die Antragsteller auf Bekleidungsbeihilfen vorrangig an Kleiderkammern der freien Wohlfahrtspflege verwiesen. Eine Barbeihilfe wird nur dann gewährt, wenn der Antragsteller die begehrten und benötigten Bekleidungsstücke in der jeweiligen Bekleidungskammer nicht erhalten kann. Zu diesem Zweck wird der Antragsteller mit einem „Laufzettel" an die Bekleidungskammer verwiesen. Auf diesem Laufzettel sind die benötigten Kleidungsstücke aufgeführt. Es sind ferner Eintragungen vorgesehen, die den Sozialleistungsträger darüber informieren, ob ein Bekleidungsstück vorhanden war und angenommen wurde, ob es vorhanden war und die Annahme verweigert wurde oder ob es nicht vorhanden war.

In Eingaben wurde beklagt, daß die Antragsteller aufgrund dieser Vorgehensweise genötigt werden, sich gegenüber den Mitarbeitern der Kleiderkammern als Sozialleistungsempfänger auszuweisen. Aufgrund der Arbeitsweise in den Kleiderkammern sei davon auszugehen, daß auch alle anderen anwesenden Personen informiert werden. Die Betroffenen würden auch namentlich als Sozialhilfeempfänger unter Nennung des Bekleidungsbedarfs aufgerufen.

Die DSK nahm hierzu wie folgt Stellung:

Nach § 4 Abs. 2 BSHG hat der Träger der Sozialhilfe über Form und Maß der Sozialhilfe nach pflichtgemäßem Ermessen zu entscheiden, soweit das Gesetz die Ermessensausübung nicht ausschließt. Zu der Frage, ob der Hilfesuchende einen generellen Anspruch auf neue Bekleidung bzw. eine die Beschaffung neuer Bekleidung ermöglichende Barbeihilfe hat oder ob der Bedarf auch durch die Abgabe einwandfreier getragener Bekleidungsstücke gedeckt werden kann, wird in der Rechtsprechung keine einheitliche Auffassung vertreten. So meint beispielsweise das OVG Lüneburg (in einem Beschluß vom 15. April 1986 – 4 B 75/86 – unter Hinweis auf Knopp/Fichtner, BSHG, 5. Auflage, RdNr. 14 zu § 12 BSHG), das Angebot, sich mit gebrauchter Kleidung zu begnügen, dürfte nur in Ausnahmefällen zulässig sein. Demzufolge dürfe ein Hilfesuchender regelmäßig nicht darauf verwiesen werden, seinen Bekleidungsbedarf bei den „Kleiderkammern" caritativer Einrichtungen zu decken.

Demgegenüber kommt das OVG Rheinland-Pfalz in einem Beschluß vom 2. Februar 1987 – 12 B 4/87 – zu dem Ergebnis, der Träger der Sozialhilfe könne den Bedarf eines Hilfeempfängers an Bekleidung durch Abgabe einwandfreier getragener Bekleidungsstücke befriedigen. In Rede stand bei dieser Entscheidung nicht die unmittelbare Übergabe von Bekleidungsstücken durch Bedienstete eines Sozialamtes, sondern ein Gutscheinverfahren.

Vor dem Hintergrund dieser letztgenannten Entscheidung geht die DSK davon aus, daß ein Sozialhilfeträger nicht ermessensfehlerhaft handelt, wenn er von einem Antragsteller verlangt, zunächst zu versuchen, den Bekleidungsbedarf bei einer Kleiderkammer zu decken.

Mit dieser Form der Leistungsgewährung muß keineswegs zwangsläufig eine Offenbarung von Sozialdaten verbunden sein; eine allgemeine Verwaltungspraxis, die sich eines „Laufzettels" als Instrument der Kontrolle – und der Datenübermittlung – bedient, wäre bedenklich. Ein Sozialhilfeempfänger, dem die benötigten Bekleidungsstücke durch die Kleiderkammer nicht zur Verfügung gestellt werden können, wird erneut beim Leistungsträger vorsprechen und eine Barbeihilfe beantragen. Im Rahmen seiner Mitwirkungspflicht nach §§ 60 ff SGB I hat er anzugeben, ob er den Versuch der Bedarfsdeckung durch die Kleiderkammer unternommen hat. Es gehört ferner zu seinen Obliegenheiten, bei berechtigten Zweifeln an der Richtigkeit seiner Angaben der Erteilung der erforderlichen Auskünfte durch Dritte (Kleiderkammern) zuzustimmen.

In Ausnahmefällen, in denen Zweifel an der Richtigkeit der Antragsangaben im Rahmen der Mitwirkung nach §§ 60 ff. SGB I nicht auszuräumen sind, ist die Offenbarung von Sozialdaten durch Anwendung des Laufzettelverfahrens nach § 69 Abs. 1 Nr. 1 SGB X zulässig, weil sie zur Hilfegewährung in einer zugelassenen Form erforderlich ist.

Im übrigen vertrat die DSK in Übereinstimmung mit dem MSF die Auffassung, daß die Abgabe der Bekleidungsstücke in den Kleiderkammern so organisiert werden muß, daß die berechtigten Belange der Betroffenen soweit wie möglich berücksichtigt werden. Es dürfte insbesondere nicht erforderlich sein, den Betroffenen namentlich als Empfänger aufzurufen, mit der Folge, daß alle übrigen in der Kleiderkammer anwesenden Personen hiervon Kenntnis erlangen. Die freien Träger der Wohlfahrtspflege sollten dafür sorgen, daß in ihren Kleiderkammern das Verfahren der Abgabe von Kleidungsstücken an Bedürftige – unabhängig davon, ob es sich um Sozialhilfeempfänger handelt oder nicht – so gestaltet wird, daß den berechtigten Diskretionsbedürfnissen der Betroffenen Rechnung getragen wird. Wo dies nicht der Fall ist, sollten die örtlichen Träger der Sozialhilfe auf

ein entsprechendes Verfahren hinwirken. Das Fehlen einer angemessenen Verfahrensweise bei der Leistungsgewährung in den Kleiderkammern ist im übrigen bei der Ermessensentscheidung über die Form der Hilfegewährung zu berücksichtigen. Es kann zur Folge haben, daß die Leistungsgewährung in dieser Form von vornherein unzulässig ist.

12.8.4 Die „Einwilligung" im Sozialleistungsverfahren

Nach der Grundsatzregelung in § 67 SGB X ist eine Offenbarung personenbezogener Daten oder von Betriebs- oder Geschäftsgeheimnissen durch Sozialleistungsträger nur zulässig, soweit der Betroffene im Einzelfalle eingewilligt hat oder soweit eine gesetzliche Offenbarungsbefugnis nach §§ 68 bis 77 SGB X vorliegt.

Die Einwilligung (vorherige Zustimmung, § 183 BGB) ist nur dann rechtswirksam, wenn sie im Einzelfalle erteilt wurde. Es muß also präzise bestimmt werden, welche Daten an wen für welche Zwecke weitergegeben werden. Pauschale Ermächtigungen genügen diesen Anforderungen nicht.

Strenge formale Anforderungen an die Einwilligungserklärung unterstreichen ihren Charakter als bewußten Willensakt des Betroffenen; zugleich dienen sie Nachweiszwecken in gerichtlichen Verfahren oder bei datenschutzrechtlichen Kontrollen. Für die Einwilligung besteht Schriftformerfordernis, von dem nur in Ausnahmefällen abgewichen werden darf. Eine besondere schriftliche Hinweispflicht auf die Einwilligungserklärung soll ausschließen, daß der Betroffene eine Einwilligungsklausel übersieht.

Alle Sorgfalt des Gesetzgebers bei der Regelung des Verfahrens kann freilich nur wenig an der Tatsache ändern, daß die Einwilligung in die Offenbarung von Sozialdaten angesichts des Angewiesenseins des Betroffenen auf Hilfeleistungen vielfach problematisch ist. So ist es beispielsweise nicht auszuschließen, daß ein Antragsteller auf Sozialleistungen mit einer Offenbarung von Informationen aus dem Antragsverfahren im Grundsatz nicht einverstanden ist, ihr aber dennoch zustimmt weil er glaubt, auf diese Weise die Antragsbearbeitung günstig beeinflussen zu können.

Die DSK versucht, einem ausufernden Rückgriff auf die Einwilligung als Zulässigkeitsvoraussetzung für die Offenbarung von Sozialdaten entgegenzuwirken. Ein Beispiel hierfür ist der folgende Fall:

Eine größere Stadt beabsichtigte, Antragsteller auf Sozialhilfe um die schriftliche Einwilligung zu bitten, die Adresse an das kommunale Energieversorgungsunternehmen weitergeben zu dürfen. Durch diese Datenweitergabe sollte das Unternehmen in die Lage versetzt werden, das Entstehen von Zahlungsrückständen rechtzeitig an den Sozialhilfeträger zu melden und diesem zu ermöglichen, dem unsachgemäßen Verbrauch der für die Bestreitung des Lebensunterhalts gewährten Barmittel zu einem frühen Zeitpunkt entgegenzuwirken. Die in der Vergangenheit dadurch jährlich entstandenen Zusatzkosten bzw. Einnahmeausfälle wurden gegenüber der DSK auf 70 000 DM beziffert.

Gegen das Verfahren waren im Grundsatz keine Einwendungen zu erheben; der zur Beurteilung vorgelegte Entwurf einer Einwilligungserklärung entsprach in materieller und formeller Hinsicht den gesetzlichen Anforderungen. Im Blick auf die Einwilligungsproblematik im Sozialleistungsverfahren forderte die DSK jedoch, nur solche Betroffene um Zustimmung zur Offenbarung von Adreßdaten zu bitten, denen tatsächlich Leistungen gewährt werden. Konkret bedeutete dies, daß der Vordruck mit der Zustimmungserklärung dem Betroffenen nicht bereits bei der Antragstellung vorgelegt, sondern dem Bescheid über die Leistungsgewährung beigefügt wird.

In einem anderen Falle ging es um die Presseberichterstattung über die Entscheidungen eines Kreisrechtsausschusses in Sozialhilfe-Widerspruchsverfahren. Ein Verband der freien Wohlfahrtspflege hatte in einer Eingabe an die DSK gerügt, daß in detaillierter Weise über die verhandelten Sachverhalte berichtet werde. Zwar werde der Name des betroffenen Sozialleistungsempfängers nicht genannt, die genaue Sachverhaltsdarstellung ermögliche aber in manchen Fällen eine Identifizierung.

Die Kreisverwaltung räumte ein, daß sie die Anwesenheit eines Presseberichterstatters in den Sitzungen des Kreisrechtsausschusses auch dann gestattet hatte, wenn Sozialhilfeangelegenheiten verhandelt wurden. In jedem einzelnen Falle sei aber der Widerspruchsführer um seine Einwilligung sowohl in die Anwesenheit eines Vertreters der Presse wie auch in die nachfolgende anonymisierte Berichterstattung gebeten worden.

Schon in ihrem 9. Tätigkeitsbericht hatte die DSK zur Öffentlichkeit der Verhandlungen in Sozialleistungs-Widerspruchsverfahren Stellung genommen (Tz. 10.1.4, S. 34). Sie hatte auf das die Verhandlungen der Rechtsausschüsse bestimmende Öffentlichkeitsprinzip hingewiesen, zugleich aber angemerkt, daß dieses Prinzip mit dem Anspruch des Betroffenen auf Wahrung des Sozialgeheimnisses kollidiert. Sie vertrat die Auffassung, der Sozialdatenschutz als Ausfluß des grundgesetzlich geschützten Persönlichkeitsrechts verdiene Vorrang vor dem Öffentlichkeitsprinzip des verwaltungsbehördlichen Vorverfahrens, das – anders als in Gerichtsverfahren – in § 16 AGVwGO lediglich durch einfaches Gesetz angeordnet sei.

Zu dem gleichen Ergebnis führt auch die Überlegung, daß der notwendige Schutz des Sozialgeheimnisses i. S. des § 16 Abs. 1 Satz 3 Halbsatz 2 AGVwGO als wichtiger Grund anzusehen ist, der in der Abwägung mit dem Öffentlichkeitsprinzip Vorrang verdient. Über die Zulassung der Öffentlichkeit ist von Amts wegen zu entscheiden; im Grundsatz ist kein Raum für eine Entscheidung, die der Einwilligung der Betroffenen maßgebliche Bedeutung beimißt. Überdies ist auch hier wieder zu beachten, daß opportunistische Erwägungen des Betroffenen die Entscheidung beeinflussen können und daß kaum ein Betroffener in der Lage sein dürfte, die Tragweite seiner Einwilligung in eine anonymisierte Berichterstattung zu überschauen. Die damit verbundenen Probleme werden oft erst dann erkannt, wenn die Bloßstellung erfolgt und nicht mehr rückgängig zu machen ist.

Im Ergebnis hält es die DSK für geboten, die Öffentlichkeit bei der Behandlung von Widersprüchen aus dem Sozialleistungsbereich auszuschließen.

12.8.5 Angabe des Verwendungszwecks auf Überweisungsvordrucken bei der Auszahlung von Sozialleistungen

In ihrem 9. Tätigkeitsbericht hatte die DSK unter Tz. 10.1.5 zu der Praxis von Sozialleistungsträgern Stellung genommen, bei der Überweisung von Sozialleistungen auf Bankkonten den genauen Verwendungszweck auf den Überweisungsvordrucken anzugeben. Im Ergebnis sah die DSK in der Angabe des Verwendungszwecks im Überweisungsverkehr zwischen Leistungsträger und Leistungsempfänger keinen Verstoß gegen die Vorschriften zum Schutze des Sozialgeheimnisses. Sie vertritt diese Auffassung auch heute noch.

Auch die vom FM bezüglich der Überweisung von Wohngeld und Leistungen des Härteausgleichs angegebenen Gründe für die genaue Kennzeichnung der Leistungen auf den Vordrucken konnten von der DSK akzeptiert werden. Im Grundsatz bestehen die gleichen Notwendigkeiten wie im sonstigen Sozialleistungsbereich. Ergänzend wies das Ministerium aber darauf hin, daß die Mitarbeiter der Geldinstitute beim Überweisungsverfahren durch beleglosen Datenträgeraustausch grundsätzlich den Inhalt von Überweisungen nicht zur Kenntnis nehmen können. Im übrigen werde bei einem Massengeschäft, wie der Wohngeldzahlung, auch bei Vermeidung der Angaben „Wohngeld" aus der Fallnummer/dem Aktenzeichen rasch ein sicherer Hinweis auf den Zahlungsgrund.

Dennoch ist den Leistungsträgern zu empfehlen, stets zu prüfen, ob die Gründe, die für eine detaillierte Angabe des Verwendungszwecks sprechen – einfache Bestimmbarkeit der Leistung für den Empfänger, Vermeidung von Verwechslungen, schnelle Identifizierbarkeit bei der Rückholung von Überweisungen wegen Änderung der Leistungsvoraussetzungen – für die einzelnen Leistungsarten noch weiterbestehen. Wenn irgend möglich, sollte eine für Außenstehende nicht bestimmbare Leistungsbezeichnung gewählt werden.

Das eigentliche datenschutzrechtliche Problem bei der Angabe des Verwendungszwecks auf Überweisungsvordrucken ist weniger darin zu sehen, daß Mitarbeiter eines Geldinstituts diese Informationen zur Kenntnis nehmen, als darin, daß diese Informationen an Kreditschutzorganisationen, Auskunfteien und ähnliche Organisationen übermittelt werden könnten. Dies wäre zwar wegen der fortgeltenden Zweckbindung nach § 78 SGB X unzulässig, gerade deshalb sollten aber organisatorische Maßnahmen zur Sicherung dieser Verpflichtung erfolgen.

12.9 Übermittlung von Aussiedlerdaten an Betreuungsorganisationen

Das Landesdurchgangswohnheim übermittelte bis zum Jahre 1982 an die in der Betreuung von Aussiedlern und Übersiedlern tätigen Organisationen und Verbände regelmäßig die persönlichen Daten der dem Land zugewiesenen und an die Landkreise und kreisfreien Städte weitergeleiteten Personen. Aufgrund datenschutzrechtlicher Bedenken wurde diese Datenweitergabe in der Folgezeit von der schriftlichen Einwilligung der Aussiedler und Übersiedler abhängig gemacht (§ 5 LDatG). Damit war die Aufgabenwahrnehmung durch die Betreuungsorganisationen allerdings in Frage gestellt, denn die Aussiedler und Übersiedler zeigten ein starkes Interesse an der Wahrung ihrer Anonymität und verweigerten in der Mehrzahl eine schriftliche Einwilligung in die Bekanntgabe personenbezogener Daten an die Organisationen und Verbände.

Es gab indessen deutliche Hinweise darauf, daß diese Verweigerung der Zustimmung keineswegs darauf zielte, Hilfsangebote zurückzuweisen. Festzustellen war vielmehr, daß die betroffenen Personen wegen der Umstellungsschwierigkeiten – in vielen Fällen auch Sprachschwierigkeiten – oft hilflos den Anforderungen der neuen Umwelt gegenüberstanden, und daß ihnen die Rechtslage nicht einsichtig war. Sie vermuteten, es gehe um Warenbestellungen oder um die Zustimmung zur Mitgliedschaft in staatlichen und nichtstaatlichen Organisationen.

Es steht außer Frage, daß die Mitwirkung von Betreuungsorganisationen bei der Eingliederung von Aussiedlern und Übersiedlern außerordentlich wichtig, in vielen Fällen für den Erfolg der Eingliederung sogar von entscheidender Bedeutung ist. Angesichts der Aufgabenstellung der Betreuungsorganisationen kann von ihrem berechtigten Interesse an der Datenübermittlung im Sinne des § 7 LDatG ausgegangen werden. Die Beeinträchtigung der schutzwürdigen Belange Betroffener ist verhältnismäßig gering, wenn die Datenübermittlung auf den Namen und die Anschrift beschränkt wird.

Nach sorgfältiger Abwägung aller Gesichtspunkte vertrat die DSK die Auffassung, daß die auf die Adreßdaten reduzierte Datenübermittlung auch dann zulässig ist, wenn die Einwilligung der Betroffenen zuvor nicht eingeholt wird.

Zugleich hielt es die DSK aber für geboten, daß das MSF nähere Bestimmungen bezüglich der als Übermittlungsempfänger zugelassenen Organisationen, über die Zweckbindung der Daten beim Empfänger sowie über die Datenlöschung trifft und den Übermittlungsempfängern eine Weitergabe der Adreßdaten an andere Personen und Stellen untersagt wird.

13 Weinbau und Weinkontrolle; Landwirtschaft

13.1 Vorbemerkung

Im 11. Tätigkeitsbericht (Tz. 14.1, 14.2) hat die DSK einen kurzen Überblick über die Meldepflichten gegeben, die von Winzern zu erfüllen sind. Sie hat die dabei maßgeblichen datenschutzrechtlichen Gesichtspunkte betont:

- Aufklärung der Winzer über Rechtsgrundlagen und Verwendungszwecke der Datenerhebungen;

- Verringerung der Belastung durch Zusammenfassung von Meldungen und Formularen;

- Wahrung der Zweckbindung der erhobenen Daten.

Es hat sich im Berichtszeitraum bestätigt, daß eine Verringerung des Umfangs der zu erhebenden Daten – das eigentliche datenschutzrechtliche Anliegen bei staatlichen Informationseingriffen – im Bereich der Landwirtschaft, insbesondere aber auch im Bereich des Weinbaus, nicht durchsetzbar ist. Dafür ist in erster Linie die EG-Weinmarktpolitik verantwortlich, die auf umfassenden Informationen über die am Weinmarkt teilnehmenden Produzenten und Händler beruht. Für die Umsetzung der EG-Anforderungen im nationalen Bereich bleibt häufig kein wesentlicher Spielraum; die EG-Rechtsgrundlagen sind sogar gegenüber bundesdeutschem Verfassungsrecht vorrangig, jedenfalls wird EG-Recht grundsätzlich vom Bundesverfassungsgericht nicht auf seine Verfassungsmäßigkeit überprüft („Solange II"-Beschluß, BVerfGE 73, 339). Damit dürfte auch eine Überprüfung hinsichtlich der Vereinbarkeit mit dem „informationellen Selbstbestimmungsrecht" des Grundgesetzes ausgeschlossen sein. In diesem Zusammenhang können grundsätzliche datenschutzrechtliche Überlegungen allein durch rechtzeitige Einflußnahme auf die EG-Gesetzgebung wirksam werden (vgl. zu den hierbei bestehenden Defiziten oben Tz. 3).

13.2 Begrenzung des Hektarhöchstertrages, EG-Weinbaukartei

Wesentlich im Berichtszeitraum war die Einführung der Hektar-Höchstmengen bei der Weinerzeugung. Voraussetzung war eine umfassende Bestandsaufnahme der von den Winzern jeweils bewirtschafteten Flächen. Im Zusammenhang mit der Einführung der EG-Weinbaukartei wurde zu diesem Zweck eine Erhebung bei den Winzern durchgeführt. Die angegebenen Daten über bewirtschaftete Flächen wurden anschließend mit dem Liegenschaftskataster bzw. dem Rebflächenverzeichnis durch die Landwirtschaftskammern abgeglichen. Dieses Verfahren beruht nach Auffassung der DSK auf ausreichenden Rechtsgrundlagen (vgl. dazu Tz. 17.2).

Im Zusammenhang mit der Begrenzung des Hektar-Höchstertrages wurden außerdem zwei Meldepflichten neu begründet (Verkehrsmeldungen sowie Meldungen von teilweise gegorenem Traubenmost, § 4 Abs. 1 sowie Abs. 2 der 5. Landesverordnung zur Durchführung des Weingesetzes). Die nicht fristgerechte und ordnungsgemäße Abgabe der Meldungen ist als Ordnungswidrigkeit mit Geldbuße bedroht.

In diesem Zusammenhang hat die DSK erreicht, daß eine strikte Zweckbindung der erhobenen Daten in der Verordnung (§ 4 Abs. 4) Ausdruck gefunden hat. Die abgegebenen Meldungen werden danach in personenbezogener Form nur zu Zwecken der Durchführung der Hektar-Höchstmengenbegrenzung, zum Zweck der Weinkontrolle sowie zu statistischen Zwecken, soweit diese auf Rechtsvorschriften beruhen, verwendet. Andere Nutzungen der Daten – etwa zu steuerrechtlichen Zwecken – sind ausgeschlossen.

Bezüglich der EG-Weinbaukartei sind nunmehr zwar die Zuständigkeiten durch Verordnung geregelt (LVO v. 1. September 1988, GVBl. S. 208), nach Auffassung der DSK fehlen jedoch nach wie vor deutliche Bestimmungen, welche Stellen zu welchen Zwecken welche Daten aus der Weinbaukartei nutzen dürfen. Sie hat das MLWF darauf hingewiesen.

13.3 Entwurf einer Weinbestandsverordnung

Der Bund hat den Ländern den Vorschlag unterbreitet, eine Verordnung zur statistischen Erhebung von Weinbeständen inländischer Herkunft zu erlassen. Hintergrund dieser Initiative ist, daß seit 1985 keine Informationen mehr darüber vorliegen, wieviel inländischer Wein in den Weinkellern lagert. Damit können keine Weinbilanzen für inländischen Wein mehr erstellt

werden. Die EG-Verordnung über Bestandsmeldungen hat eine nationale Ertassung des Weinbestandes in diesem Zusammenhang nicht für erforderlich gehalten und deshalb von entsprechenden Datenerhebungen abgesehen.

Aus Sicht der DSK ist die Begründung für die Einführung einer weiteren Meldung, die die Winzer belastet, nicht zwingend: Wenn die EG, der im Weinsektor die maßgebliche Rechtsetzung zugefallen ist, entsprechende Informationen für entbehrlich hält, spricht die Vermutung zunächst gegen die zwingende Erforderlichkeit einer solchen Datenerhebung auf nationaler Ebene. Es kommt hinzu, daß nach Auffassung der DSK die beabsichtigte Statistik nicht im Verordnungwege (gem. § 5 Abs. 2 Bundesstatistikgesetz), sondern nur durch ein formelles Gesetz begründet werden könnte. Hintergrund des genannten Informationsbedürfnisses ist nämlich kein konkreter, im Zeitpunkt der Erhebung schon festliegender Bundeszweck. Dies wäre aber Voraussetzung, um die Verordnungsermächtigung des § 5 Abs. 2 Bundesstatistikgesetz nutzen zu können.

Die DSK hat das zuständige Ministerium über diese Überlegungen unterrichtet.

13.4 Zentralstelle für Weinüberwachung

In Weiterführung der Initiativen zur Schaffung einer gesetzlichen Grundlage für die Einrichtung einer Zentralstelle für Weinüberwachung und für deren Aufgabenzuweisung – die DSK berichtete über das Vorhaben bereits in ihrem 11. Tätigkeitsbericht Tz. 14.3 – legte das MUG im November 1988 einen vom Ministerrat in den Grundzügen gebilligten Gesetzentwurf zur Stellungnahme vor.

Die beabsichtigte Konzentration der Datenverarbeitung zum Zwecke der Weinüberwachung bei einer Zentralstelle ist aus der Sicht der DSK nach wie vor von erheblichem datenschutzrechtlichem und datenschutzpolitischem Gewicht. Eindeutig unzulässig wäre das Vorhaben indessen nur dann, wenn mit der Datenübermittlung an die Zentralstelle auch eine Zweckänderung der Daten verbunden wäre. Dies ist aber nach den Darlegungen des Ministeriums nicht der Fall.

Die DSK empfahl mehrere Verbesserungen im Detail.

Im Landtag wurde der Gesetzentwurf bisher nicht eingebracht; ob das Projekt noch weiterverfolgt wird, ist nicht bekannt.

14 Steuern und kommunale Abgaben

14.1 Zum Stand der Automation in der Finanzverwaltung und zu den Aufgaben der DSK in diesem Bereich

Durch das Vordringen der automatisierten Datenverarbeitung im Bereich der Abgabenerhebung sind eine Reihe verfassungsrechtlicher und gesetzlicher Anforderungen ergänzend zum klassischen Steuergeheimnis hinzugetreten, die es aus Sicht der DSK erfordert haben, auch diesem Bereich vermehrt Aufmerksamkeit zu widmen. Folgende technische Entwicklungen stehen hierbei im Vordergrund:

– Zentrale automatisierte Datenspeicherung bez. der Steuerpflichtigen

Nahezu jeder Bedienstete in der Finanzverwaltung hat Zugang zu einem Terminal, der Zugriff auf zentrale Datenbestände der „Zentrale für Datenverarbeitung der Finanzverwaltung" (ZDFin) in Koblenz ermöglicht. Schon die daraus folgenden Informationsmöglichkeiten und, als Korrektiv, die Anforderungen an die Gestaltung der Verfahren (insbesondere: Beschränkung und effektive Sicherung der Zugriffsmöglichkeiten) rechtfertigen die aufmerksame Beobachtung durch die Datenschutzkontrolle (zum Entwicklungs- und Planungsstand der zentralen Datenverarbeitung in der Finanzverwaltung kann auf eine recht ausführliche veröffentlichte Ausarbeitung des Leiters der ZDFin, Abt. Dir. Jäger, verwiesen werden: DV in der Finanzverwaltung, in Datenverarbeitung, Steuer, Wirtschaft, Recht 1988, S. 127-135).

– Einführung von Dialogverfahren in den Finanzämtern

Hinzu kommt, daß die Nutzer dieser Terminals im Zuge der jüngsten Entwicklung nicht mehr nur Daten zum Zweck ihrer Kenntnisnahme abrufen können: sie können zunehmend auch unmittelbar Veränderungen im Datenbestand bewirken. Die damit gegebenen (theoretisch vorstellbaren) Mißbrauchsmöglichkeiten erfordern erhöhte Aufmerksamkeit aller an dieser Verfahrenseinführung Beteiligten, aber auch der unabhängigen Datenschutzkontrolle (zu den Auswertungsmöglichkeiten, die das von der ZDFin eingesetzte System „DAVID" bietet, vgl. Jäger, a. a. O., S. 130).

– Einsatz von Arbeitsplatzcomputern

Insbesondere in den Prüfungsbereichen der Finanzverwaltung (Betriebsprüfung, Steuerfahndung) ist ein Vordringen des Einsatzes von Arbeitsplatzcomputern (PC) zu konstatieren. Dabei werden z. Z. in einem vielfach höheren Maß private als dienst-

liche Geräte eingesetzt. Die damit gegebenen technischen Möglichkeiten führen zu zusätzlichen Gefährdungen des informationellen Selbstbestimmungrechts der betroffenen Steuerpflichtigen. Auch unter diesem Aspekt sieht sich die DSK veranlaßt, diesem Bereich, in dem äußerst sensible Informationen erhoben und verarbeitet werden, verstärkte Aufmerksamkeit zu widmen.

– Auswirkungen der Automation auf das Steuergeheimnis

Die vorgenannten technischen Neuentwicklungen haben unter datenschutzrechtlichem Aspekt Einfluß auf die Frage, ob das informationelle Selbstbestimmungrecht der Steuerpflichtigen auch bei herkömmlichen Datenverarbeitungsmethoden in Steuerangelegenheiten angemessen gewahrt wird. So ist die Frage, welche Informationen unter welchen Voraussetzungen durch wen an andere öffentliche oder private Stellen weitergegeben werden dürfen, dann von ungleich größerer datenschutzrechtlicher Relevanz, wenn die Informationsmöglichkeiten des übermittelnden Sachbearbeiters durch die technikunterstützte Nutzung zentral gespeicherter Informationen im Vergleich zum traditionellen Verwaltungsverfahren inkommensurabel gesteigert sind.

14.2 Zur Kooperation mit der Finanzverwaltung

Vor diesem Hintergrund bedauert die DSK, daß mehrere Konfliktpunkte mit dem Ministerium der Finanzen nicht ausgeräumt werden konnten.

– Der DSK wurde in weiten Bereichen die Prüfkompetenz für Vorgänge, die datenschutzrechtlich bedeutsam sind, bestritten (dazu unten 14.2.1).

– Die der DSK gem. § 20 LDatG zu leistende Unterstützung wurde teilweise nur zögerlich gewährt (dazu unten 14.2.2).

– Anmeldungen automatisierter Verfahren, die gem. § 10 LDatG vorzunehmen sind, erfolgten zu spät oder gar nicht (dazu unten 14.2.3).

14.2.1 Prüfkompetenz der DSK

Wie die Finanzverwaltungen anderer Bundesländer hat auch das Finanzministerium in folgenden drei Fallgruppen die Kompetenz der Datenschutzkontrollinstitution bestritten und ihr dementsprechend auch die Unterstützung verweigert:

a) in den Fällen, in denen die DSK die Rechtmäßigkeit der Datenerhebung überprüfen wollte (Tz 14.2.1.1),

b) in den Fällen, in denen die DSK die Einhaltung datenschutzrechtlicher Bestimmungen im Zusammenhang mit traditionellen Datenverarbeitungsmethoden überprüfen wollte (z. B. bei der Übermittlung von Daten aus Akten, Tz. 14.2.1.2),

c) in den Fällen, in denen die DSK systematische Kontrollen der automatisierten Datenverarbeitung bei der Finanzverwaltung durchführen wollte und dabei (notwendigerweise) Kenntnis von personenbezogenen Daten Steuerpflichtiger erhalten mußte (Tz. 14.2.1.3).

Zur Zeit scheint sich jedoch (bezüglich der Fallgruppen 14.2.1.1 und 14.2.1.2) ein gewisser Wandel anzubahnen, der künftig eine effektivere Zusammenarbeit erhoffen läßt.

Zu den einzelnen Fallgruppen:

14.2.1.1 Prüfung der Datenerhebung

Die Erhebung von Daten beim betroffenen Steuerpflichtigen oder auch bei Dritten (anderen öffentlichen Stellen, anderen Privatpersonen) ist in der Abgabenordnung an verschiedenen Stellen gesetzlich geregelt (z. B. §§ 93, 97 AO). In der Praxis wenden sich Beschwerdeführer an die DSK und bemängeln beispielsweise, daß die Finanzbehörden sich ungerechtfertigterweise bei Dritten über ihre privaten Verhältnisse erkundigt hätten. Aber auch andere öffentliche Stellen (etwa Gemeinden oder Kreisverwaltungen) fragen bei der DSK an, ob sie verpflichtet sind, auf bestimmte Fragen der Finanzverwaltung Auskünfte zu erteilen.

Die DSK geht davon aus, daß ihr auch in diesen Fällen ein uneingeschränktes Prüfungsrecht zusteht. Bei den genannten Regelungen der Abgabenordnung handelt es sich um „andere Vorschriften über den Datenschutz" im Sinne des § 17 Abs. 1 LDatG. Die Überwachung der Einhaltung dieser anderen Vorschriften über den Datenschutz ist ihr vom Gesetzgeber anvertraut worden. Derartige Prüfungen sind auch sinnvoll, weil in den meisten Fällen die erhobenen Daten automatisiert weiterver-

arbeitet werden: Sie gehen in der einen oder anderen Form in die automatisierte Datenverarbeitung (z. B. Steuerberechnungsverfahren) ein. Die DSK hatte auch wiederholt Veranlassung, insoweit eine zu großzügige Auffassung der Finanzverwaltung, was die Tragweite der gesetzlichen Bestimmungen betrifft, festzustellen (s. dazu Tz. 14.7).

Hierzu hat das Finanzministerium allerdings in einer grundsätzlichen Stellungnahme vom 8. November 1989 (Az. S 0130 A – 441) seine Bereitschaft bekundet, im Interesse einer reibungslosen Zusammenarbeit und im Vorgriff auf die im BDSG-Entwurf beabsichtigte Regelung folgendes Verfahren zu akzeptieren: Wenn eine konkrete Beschwerde eines Steuerpflichtigen vorliege, die die Verletzung datenschutzrechtlicher Vorschriften möglich erscheinen lasse, und wenn das Steuergeheimnis Dritter nicht berührt sei, sei die Finanzveraltung bereit, konkrete Auskünfte auf Anfrage zu erteilen.

Übergangsweise kann die DSK diesem Vorschlag als Minimallösung zur Durchführung ihrer gesetzlichen Aufgaben zustimmen.

14.2.1.2 Zur Prüfkompetenz beim Umgang mit Daten in herkömmlicher Form

Hier wird der DSK beispielsweise die Kompetenz bestritten, Eingaben nachzugehen, in denen Beschwerdeführer die Übermittlung von Daten aus ihren Steuerakten bemängeln. Die Bedeutung dieser Beschränkung wird zwar zunehmend geringer, da die wesentlichen Informationen aus den Steuerakten in automatisierter Form gespeichert werden. Andererseits gibt es eine Reihe von Nachweisen und tatsächlichen Vorgängen, die nur in herkömmlicher Form in Akten gespeichert werden (beispielsweise der Inhalt von ärztlichen Attesten). Die Frage, unter welchen Voraussetzungen Auskünfte aus Akten an andere Personen oder Stellen erteilt werden dürfen, darf nach Auffassung des Finanzministeriums von der DSK nicht überprüft werden. In entsprechenden Fällen verweigerte sie bislang ihre Unterstützung zur Aufklärung. Der Rechtsstandpunkt der DSK hierzu ergibt sich aus den Ausführungen zu Tz. 14.2.1.1:
Auch das Steuergeheimnis, § 30 AO, ist eine „andere Vorschrift über den Datenschutz". Unter den gleichen Voraussetzungen wie oben zu Tz. 14.2.1.1 geschildert, dürfte auch in diesem Zusammenhang künftig eine Lösung der konkreten Problemfälle möglich sein.

14.2.1.3 Einschränkungen bei der Kontrolle automatisierter Verfahren innerhalb der Finanzverwaltung

Eine umfassende Prüfung, ob technische Sicherungsmaßnahmen tatsächlich vor Ort bei den einzelnen Finanzämtern und innerhalb der ZDFin eingehalten werden, setzt voraus, daß unangemeldete stichprobenartige Prüfungen durchgeführt werden können. Diese müssen sich z. B. darauf beziehen, ob datenschutzrechtlichen Anforderungen beim Zugriff auf die Datenbestände Rechnung getragen wird. Dabei ist es zwingend erforderlich, die Datenverarbeitungsgeräte „in Tätigkeit" zur Kenntnis zu nehmen. Auch die Funktionstüchtigkeit von entsprechenden Zugriffsbeschränkungen kann nur dann geprüft werden, wenn sie im Echtverfahren getestet werden können; dabei werden zwangsläufig personenbezogene Daten von Steuerpflichtigen der prüfenden Stelle (der DSK) bekannt. Das Finanzministerium steht auf dem Standpunkt, daß das Steuergeheimnis derartige Prüfungsmaßnahmen der DSK verbiete. Dies ist nach Auffassung der DSK nicht zutreffend und beeinträchtigt ihre Wirkungsmöglichkeiten im Bereich der Finanzverwaltung empfindlich:
Gleichermaßen wie dem Rechnungshof eine Prüfkompetenz bez. der ordnungsgemäßen Verwaltung und Verwendung öffentlicher Mittel zusteht, die vom Steuergeheimnis nicht eingeschränkt wird, steht der DSK eine entsprechende Prüfkompetenz bez. der Ordnungsmäßigkeit der Datenverarbeitung zu. Sie ist insofern als staatliche Stelle Teil des Aufsichtsstranges und nimmt aufgrund einer besonderen gesetzlichen Zuständigkeits- und Befugniszuweisung (§§ 17, 20 LDatG) ihre Aufgaben wahr. Durch die genannten datenschutzrechtlichen Regelungen wird § 30 AO zulässigerweise konkretisiert. Dabei ist zu beachten, daß diese Konkretisierung im Interesse einer effektiven Sicherung des informationellen Selbstbestimmungsrechts der betroffenen Steuerpflichtigen erfolgt. Es handelt sich hierbei nicht um zielgerichtete Eingriffe in Rechte der Betroffenen, sondern vielmehr um Maßnahmen, um die Rechte der Betroffenen entsprechend den verfassungsrechtlichen Vorgaben angemessen zu sichern.

Eine praktische Lösung dieser Streitfrage ist vor Erlaß der Neufassung des BDSG nicht in Sicht, zumal fast alle Finanzverwaltungen in der Bundesrepublik die Rechtsauffassung der DSB/DSK ablehnen.

14.2.2 Zögerliche Unterstützungsleistungen

Aber auch in den Fällen, in denen die Prüf- und Beratungskompetenz der DSK zweifelsfrei ist, leistete das Finanzministerium häufig die gem. § 20 LDatG vorgeschriebene Unterstützung nur zögerlich.

In Konkretisierung der gesetzlichen Regelung (§§ 17, 20 LDatG) ist der DSK von den Ministerien vor der Entscheidung über Datenschutzprobleme von allgemeiner Bedeutung Gelegenheit zur Stellungnahme zu geben. Sie ist frühzeitig über Datenschutzprobleme von grundsätzlicher Bedeutung zu unterrichten, außerdem soll ihr rechtzeitig Gelegenheit gegeben werden,

zu Entwürfen von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften, die Regelungen für die Verarbeitung personenbezogener Daten treffen, Stellung zu nehmen (dies hat, auf ein Ersuchen der DSK hin, die Konferenz der Staatssekretäre beschlossen; dieser Beschluß ist in den einzelnen Ministerien in Hausverfügungen umgesetzt worden).

In diesem Bereich hat es Probleme gegeben; in einem Fall hat das Finanzministerium zunächst sogar auf konkrete Anforderung hin die Vorlage einer Verwaltungsvorschrift verweigert (s. Tz. 14.2.2.2).

14.2.2.1 Verwaltungsanweisung über den Einsatz privater PC

Beispielsweise wurde für den Bereich des gesamten Landes durch die Oberfinanzdirektion Koblenz eine Verwaltungsverfügung über den Einsatz privater Personalcomputer in Finanzämtern erlassen. Die erste entsprechende Verfügung datiert vom 10. Juli 1985; sie wurde 1986 geändert und am 1. März 1988 durch eine neue Verfügung weitgehend ersetzt.

Die DSK erhielt erst aufgrund örtlicher Feststellungen am 20. Dezember 1988 von der Existenz dieser Verfügungen Kenntnis. Angesichts der Tatsache, daß unter datenschutzrechtlichen Gesichtspunkten die genannten Regelungen ergänzungsbedürftig sind, sieht die DSK darin eine den Datenschutzstandard im Finanzbereich beeinträchtigende Unterlassung.

14.2.2.2 Verwaltungsanweisung über Erledigung von Auskunftsersuchen des Verfassungsschutzes

Mit Datum vom 28. März 1979 wurde eine allgemeine Weisung durch das FM an die Finanzämter erlassen, die das Verfahren zur Erledigung von Auskunftsersuchen des Verfassungsschutzes durch Finanzämter regelt. Die DSK erhielt von der Existenz dieser Verwaltungsanweisung im Juli 1987 ohne Zutun der zuständigen Ressorts Kenntnis. Ihre Bitte, ihr diese Verwaltungsvorschrift vorzulegen, wurde zunächst mit dem Argument abgelehnt, es sei kein Grund dafür zu erkennen, wie ein solches Verlangen nach Vorlage der Verwaltungsanweisung gerechtfertigt werden könnte, da ihr Inhalt der DSK inzwischen schriftlich dargelegt worden sei.

Erst nach einem ausführlichen Schriftwechsel und nach einem eingehenden Gespräch auf Ministerebene hat das FM sich im September 1988 grundsätzlich mit einer Diskussion auf Basis des Wortlauts der angesprochenen ministeriellen Anweisung bereiterklärt. Dies war aus datenschutzrechtlicher Sicht auch erforderlich, da die vorher gegebene schriftliche Darstellung des Inhalts der Verwaltungsanweisung dem tatsächlichen Wortlaut dieser Anweisung an datenschutzrechtlich bedeutsamen Punkten nicht voll entsprochen hat.

Es hat in diesem Fall also ca. 1 ½ Jahre gedauert, bis allein die an sich selbstverständliche Vorlage einer Verwaltungsanweisung bei der DSK durchgesetzt werden konnte. Kompetenzprobleme konnte es in diesem Zusammenhang nicht geben, da die angesprochene Verfügung auch die Übermittlung von Daten aus dem automatisierten Verfahren der Finanzverwaltung regelt.

14.2.2.3 Vorgänge auf Bundesebene

Ergänzend ist darauf hinzuweisen, daß auch – entgegen der oben angesprochenen allgemeinen Absprache – das FM es in der Vergangenheit häufiger unterlassen hat, Referentenentwürfe von datenschutzrechtlich bedeutsamen Rechtssetzungsverfahren auf Bundesebene (seien es Gesetzentwürfe oder Verordnungsentwürfe) der DSK von Amts wegen zu übermitteln. Häufig hat sie diese nur erhalten, wenn sie über den Bundesbeauftragten für den Datenschutz oder über andere Landesbeauftragte von der Existenz entsprechender Entwürfe Kenntnis erhielt und entsprechende Bitten an das FM richtete. Vor dem Hintergrund der inzwischen erkennbaren Kooperationsbereitschaft erwartet die DSK allerdings künftig eine Verbesserung.

14.2.2.4 Verzögerungen bei der Antworterteilung durch Finanzämter

Wenn die DSK konkreten Bürgerbeschwerden nachgeht, befragt sie üblicherweise zunächst unmittelbar das betroffene Finanzamt. Wiederholt haben die Antworten auf die im Regelfall leicht zu beantwortenden Fragen die DSK erst mit einer Zeitverzögerung von ca. 8 – 12 Wochen erreicht. Grund dafür ist, daß die Antworten fast ausnahmslos auf dem Dienstweg (über die Oberfinanzdirektion Koblenz sowie das FM) an die DSK gerichtet werden. Die DSK hegt allerdings die Erwartung, daß aufgrund der seit kurzem feststellbaren Kompromißbereitschaft des FM künftig auch diese Verfahrensfrage gelöst wird und eine schnellere Beantwortung von Anfragen möglich wird.

14.2.3 Anmeldungen automatisierter Verfahren gem. § 10 LDatG

Nach dem LDatG haben die öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, die Pflicht, die entsprechenden Verfahren („Anwendungen") bei der DSK anzumelden. Solange nur zentrale Verfahren durch die ZDFin eingeführt worden sind, wurde diese Anmeldepflicht zentral durch das FM erfüllt. Schon in diesem Zusammenhang hat die DSK zwar zu bemängeln, daß für die Abrufverfahren vor Ort keine ausreichenden Sicherungsmaßnahmen in Dienstanweisungen auf der Ebene der einzelnen Finanzämter vorgelegt worden sind. Abgesehen davon lief das Anmeldungsverfahren in diesem Zusammenhang jedoch zufriedenstellend.

Nachdem aber dezentrale Verfahren oder auch Pilotverfahren eingeführt sind, die nur in einzelnen Finanzämtern praktiziert werden, ist die Anmeldepraxis z. T. unbefriedigend: die DSK besitzt trotz mehrfacher Versuche, Klarheit zu gewinnen, keinen umfassenden und genauen Überblick über den Einsatz der automatisierten Datenverarbeitung bei den einzelnen Finanzämtern. Sie entnahm dem Rahmenplan der ZDFin 1988/1989 (erstellt mit Datum vom Juni 1987, zugegangen am 20. Oktober 1987), daß für die Einheitsbewertung des Grundbesitzes ein neues Rahmenprogramm entwickelt worden sei. Die Erprobung sei bei den Finanzämtern Trier und Mayen erfolgt. Aufgrund der Erfahrungsberichte der beiden Ämter habe das FM die Zustimmung zur Übernahme bei den übrigen Finanzämtern erteilt.

Die Erprobung der entsprechenden Verfahren ist mit Echtdaten erfolgt. Dann aber war bereits diese Datenverarbeitung anmeldepflichtig, da das LDatG keine Privilegierung von „Erprobungsverfahren" kennt, die mit Daten betroffener Bürger arbeiten. Es ist nicht gerechtfertigt, den Schutz des Bürgers zu vernachlässigen, auch wenn sich DV-Verfahren erst in der Erprobung befinden. Soll die DV zunächst unbelastet von datenschutzrechtlichen Anforderungen stattfinden, so ist mit „Spielmaterial" oder fiktiven Daten zu arbeiten. Bei dem genannten Einheitsbewertungsverfahren wurde die DSK weder über die Erprobungsphase noch, nach deren Abschluß, rechtzeitig über die flächendeckende Einführung informiert. Die förmliche Anmeldung bei der DSK erfolgte vielmehr erst mit Schreiben vom 9. Dezember 1988.

Wesentliche Veränderungen wurden bezüglich des dialogorientierten Festsetzungsverfahrens im System DAVID eingeführt. Eine Anmeldung des Versuchs, der ebenfalls mit Echtdaten stattgefunden hat, ist bei der DSK nicht erfolgt.

Es wurde der DSK nicht einmal mitgeteilt, welche Finanzämter zunächst an diesen Verfahren teilgenommen haben.

Die DSK hat auch das Unterlassen der Anmeldungen bei der Einführung von Personalcomputern im Rahmen der Betriebsprüfung sowie der Steuerfahndung zu beanstanden. Nach ihren Feststellungen bei einer örtlichen Prüfung wurden seit Ende 1987 bei Betriebsprüfungsstellen in Mainz und Ludwigshafen sowie bei einer Steuerfahndungsstelle Personalcomputer eingesetzt. Diese haben von Beginn an auch mit personenbezogenen Daten von Steuerpflichtigen gearbeitet. Eine den PC-Einsatz betreffende Anfrage vom April 1988, wurde trotz Erinnerung im September erst mit Schreiben vom 9. Dezember 1988 beantwortet. Zur Frage, welche Datenarten gespeichert werden und zum Verwendungszweck (dies sind die wichtigsten Merkmale einer Anmeldung nach § 10 LDatG) wurden jedoch keine Ausführungen gemacht. Eine Ergänzung erfolgte erst mit Schreiben vom 13. Februar 1989. In diesem Zusammenhang ist weiter zu bemängeln, daß seit mehreren Jahren Personalcomputer im Einsatz sind und mit personenbezogenen Daten arbeiten, ohne daß auf Finanzamtsebene verbindliche konkrete Regelungen über Sicherungsmaßnahmen bestanden (vorgeschrieben durch § 9 Abs. 2 LDatG).

14.3 Kontrollmitteilungsverordnung

Seit langem wurde von den Datenschutzbeauftragten gefordert, daß sogenannte „Kontrollmitteilungen" (Mitteilungen anderer öffentlicher Stellen über die Zahlung von Geldern an private Empfänger an das Wohnsitzfinanzamt des Empfängers) auf eine gesetzliche Grundlage zu stellen sind. Dieser Forderung ist der Bundesgesetzgeber im Grundsatz durch Einfügung des § 93 a AO nachgekommen (mit Gesetz vom 19. Dezember 1985).

Diese Vorschrift beinhaltet jedoch nur eine Ermächtigungsgrundlage zum Erlaß einer Bundesrechtsverordnung. Das Kontrollmitteilungsverfahren wäre nur dann gesetzlich zulässig, wenn die dazugehörige Verordnung erlassen worden wäre. Dies ist bislang nicht der Fall. Entwürfe wurden zwar diskutiert (und auf Anforderung der DSK zur Verfügung gestellt), entscheidende Fortschritte bei der Verabschiedung sind jedoch nicht ersichtlich. Das FM sollte aus Sicht der DSK alle Anstrengungen unternehmen, um diese wesentliche Frage datenschutzrechtlich einwandfrei zu lösen: Wenn die erwähnte Rechtsverordnung nicht verabschiedet wird, käme in Betracht, die Anforderung von Kontrollmitteilungen auszusetzen. Dies ist in Bremen und in Hessen bereits erfolgt. Nur so kann vermieden werden, daß die DSK das Kontrollmitteilungsverfahren wegen des Fehlens der erforderlichen Rechtsgrundlage beanstandet.

14.4 Steuerdatenabrufverordnung

Ebenfalls mit Gesetz vom 19. Dezember 1985 wurde die Regelung über das Steuergeheimnis um Anforderungen an automatisierte Abrufverfahren innerhalb der Finanzverwaltung ergänzt. Auch diese gesetzlichen Anforderungen sind durch eine Rechtsverordnung zu konkretisieren. Der entsprechende Entwurf einer „Steuerdatenabrufverordnung" liegt bereits seit längerem vor. Stellungnahmen der Datenschutzbeauftragten dazu wurden zeitnah abgegeben. Auch hier sollte das FM alle ihm gegebenen Möglichkeiten der Einflußnahme auf den Bund ausschöpfen, die Verabschiedung der Verordnung – die aus datenschutzrechtlicher Sicht grundsätzlich bedeutsam ist – zu beschleunigen.

14.5 Datenübermittlungen zum Zweck gemeindlicher Steuerfestsetzungen

Die DSK hat wiederholt das in § 184 Abs. 3 AO vorgeschriebene Datenübermittlungsverfahren an Gemeinden unter verfassungsrechtlichen Gesichtspunkten gerügt. Diese Vorschrift wurde mit Gesetz vom 19. Dezember 1985 auf Betreiben einiger Bundesländer eingefügt. Danach haben die Finanzbehörden den Inhalt z. B. des Gewerbesteuermeßbescheids den Gemeinden mitzuteilen, denen dann die Steuerfestsetzung obliegt. Die Mitteilung des gesamten Gewerbesteuermeßbescheides ist für die Gemeinden in Rheinland-Pfalz zur Festsetzung der Steuer nicht erforderlich. Hier reicht es aus – wie es in der Vergangenheit auch gesetzlich geregelt war –, daß die Gemeinden den Steuermeßbetrag erfahren, nicht aber die Faktoren, die zu seiner Berechnung geführt haben. Mit der umfassenden Datenübermittlung werden schützenswerte Belange der betroffenen Gewerbebetreibenden verletzt; Informationen über ihre wirtschaftliche Lage gelangen an die Verbandsgemeinden, die diese Informationen zur Steuerfestsetzung im einzelnen nicht benötigen.

Das Finanzministerium hat auf das entsprechende Anliegen der DSK mit der Antwort reagiert, eine Initiative zur Änderung dieser Regelung erscheine wenig aussichtsreich. Aus Sicht der DSK entspricht diese Reaktion nicht der Bedeutung der angesprochenen Frage.

14.6 Gesetz zu einer abschließenden datenschutzrechtlichen Regelung in der Abgabenordnung

Im Berichtszeitraum ist auf Anregung der Länder ein Referentenentwurf zur Ergänzung der Abgabenordnung um datenschutzrechtliche Vorschriften entstanden, der aus datenschutzrechtlicher Sicht auf erhebliche Kritik gestoßen ist. Die Entwurfsverfasser hatten beabsichtigt, die Geltung der Datenschutzgesetze im Steuerbereich völlig auszuschließen und eine umfassende bereichsspezifische Regelung in die AO aufzunehmen.

Abgesehen davon, daß es kaum sinnvoll erscheint, organisatorische und technische Maßnahmen der Datensicherung, die für jede automatisierte Verarbeitung personenbezogener Daten Bedeutung haben, oder Befugnisse der Datenschutzkontrolle bereichsspezifisch zu regeln, war an dem vorgelegten Entwurf besonders zu kritisieren, daß nicht nur die Datenerhebung, sondern auch jede Datenübermittlung von der Prüfkompetenz der Datenschutzbeauftragten (bzw. der DSK) ausgenommen sein sollte.

Diese und andere Kritikpunkte, die von allen Datenschutzbeauftragten gemeinsam vorgetragen wurden, haben schließlich dazu geführt, daß der genannte Referentenentwurf nicht weiter verfolgt wird.

Die DSK sieht in dieser Entscheidung der Finanzverwaltungen ein Zeichen für eine zunehmend sachangemessene Einstellung gegenüber den datenschutzrechtlichen Erfordernissen.

14.7 Einzelfragen aus dem Steuer- und Abgabenbereich

14.7.1 Wahrung des Steuergeheimnisses bei telefonischen Auskünften

Aufgrund einer Eingabe erfuhr die DSK, daß ein Finanzamtsmitarbeiter Auskünfte aus einem Steuerfall über noch offene Steuerschulden und gezahlte Steuern an eine unberechtigte Person telefonisch erteilt hat.

Der Sachverhalt wurde vom betroffenen Finanzamt eingeräumt. Der zuständige Bedienstete erkärte jedoch, der Anrufer habe die zutreffende Steuernummer genannt und sich auch ansonsten durch Kenntnisse des Steuerfalles ausgewiesen.

Die DSK hat dazu ausgeführt, daß unter Berücksichtigung des Gewichts der telefonisch gestellten Fragen – nach der Tatsache der Zahlung der Einkommensteuer, nach der Bank und der Kontonummer, von wo das Geld abgebucht worden ist – diese Gesichtspunkte zur Identitätsfeststellung des Anrufers ausgereicht haben. Die DSK hat es in Übereinstimmung mit dem FM für unverhältnismäßig gehalten, für Fragen der in Rede stehenden Art jeden Anrufer auf den schriftlichen Weg zu verweisen. Als Konsequenz wäre eine telefonische Erörterung von steuerlichen Fragen auch geringerer Bedeutung zwischen den Sachbearbeitern des Finanzamts und Steuerpflichtigen nicht mehr möglich. Dies wäre eine nicht akzeptable Überbetonung von Vorsichtsmaßnahmen. Dennoch sollten Fälle wie der geschilderte dazu Veranlassung geben, bei Zweifeln an der Identität des Anrufers geeignete Maßnahmen zu ergreifen.

14.7.2 Aufbewahrung von ärztlichen Gutachten bei Versicherungen zu steuerlichen Zwecken (§ 147 AO)

Nachdem ein Bürger den Abschluß eines Lebensversicherungsvertrages beantragt hatte und zu diesem Zweck in die Anfertigung ärztlicher Gutachten eingewilligt hatte, die der Lebensversicherung zur Verfügung gestellt wurden, kam kein Vertrag zustande. Die Lebensversicherung hatte Bedingungen gestellt, mit denen der antragstellende Bürger nicht einverstanden war. Daraufhin verlangte er, daß die ärztlichen Gutachten bei der Lebensversicherung an ihn ausgehändigt und alle Informationen

über den Inhalt dieser Gutachten bei der Lebensversicherung gelöscht werden. Die Versicherungsgesellschaft antwortete, daß sie aus steuerlichen Gründen (gem. § 147 Abgabenordnung) zur Aufbewahrung auch solcher Gutachten für sechs Jahre verpflichtet sei.

Die DSK konnte dem nicht beipflichten. Nach der genannten Vorschrift sind nur solche Unterlagen beim Steuerpflichtigen aufzubewahren, die Bestandteile der Buchführung sind. Im vorliegenden Zusammenhang wären das die Rechnungen der Gutachter, nicht dagegen die Gutachten im Wortlaut.

Im Grundsatz hat das FM dieser Auffassung zugestimmt.

Die DSK hat den Beschwerdeführer entsprechend unterrichtet: Sie mußte ihn jedoch auch darauf hinweisen, daß er seine Ansprüche auf Herausgabe bzw. Vernichtung der entsprechenden Unterlagen nur auf dem Zivilrechtsweg – ggf. unter Zuhilfenahme der Gerichte – durchsetzen könne, da die DSK keine unmittelbaren Einwirkungsmöglichkeiten auf private Stellen besitzt.

14.7.3 Beschäftigung von Schülern als Praktikanten bei Finanzämtern

In den Abschlußklassen der Hauptschulen, aber auch in vergleichbaren Klassenstufen der Realschulen und Gymnasien, werden Schülerpraktika durchgeführt. Sie sollen dazu dienen, die Schüler mit dem Berufsleben vertraut zu machen und ihnen die Möglichkeit eröffnen, die gewonnenen Erfahrungen strukturiert im Unterricht aufzuarbeiten. Diese Praktika dauern 14 Tage; sie werden hauptsächlich in privaten Unternehmen, aber auch – in geringerem Umfang – in der öffentlichen Verwaltung durchgeführt.

Ein Finanzamtsbediensteter, der bei der Finanzkasse mit Hilfe seines EDV-Terminals Zugriff auf nahezu alle Steuerkonten seines Finanzamtsbezirks hat, beschwerte sich bei der DSK darüber, daß auch in seinem Finanzamt Schülerpraktikanten beschäftigt waren, die vom Steuergeheimnis geschützte Daten unter Nutzung der EDV-Terminals zur Kenntnis nehmen konnten. Seine eigenen Versuche, diese Frage innerhalb seines Finanzamts zu bereinigen, waren erfolglos geblieben.

Die DSK nahm diese Eingabe zum Anlaß, gegenüber der OFD und dem Finanzministerium die Frage des ausreichenden Schutzes des Steuergeheimnisses auch in diesem Zusammenhang zu erörtern.

Bemerkenswert ist, daß das FM unter dem Gesichtspunkt des Steuergeheimnisses keine grundsätzlichen Bedenken gegen die Offenbarung entsprechender Daten an Praktikanten hatte. Seine Bedenken knüpften sich daran, daß die Schüler nicht wirksam dazu verpflichtet werden könnten, wie Amtsträger das Steuergeheimnis zu wahren.

Diese Auffassung ist deshalb schwer verständlich, weil die Beauftragten und die Mitglieder der DSK, die zweifelsfrei Amtsträger sind und als solche die bei Prüfungsmaßnahmen zur Kenntnis genommenen Steuerdaten geheimzuhalten haben (und sich bei Verstoß gegen diese Pflicht strafbar machen würden), nach Auffassung des Ministeriums keine entsprechenden Daten zur Kenntnis nehmen dürfen, weil das Steuergeheimnis entgegenstände. Dazu wurde oben (Tz. 14.2.1.3) bereits inhaltlich Stellung genommen.

Bezüglich der Schülerpraktikanten hat das FM jedoch keine vergleichbaren Bedenken. Im Ergebnis hat es sich dennoch der Auffassung der DSK angeschlossen, daß deren Beschäftigung in Finanzämtern nicht zulässig ist. Maßgeblich für das FM war dabei die Überlegung, daß eine wirksame Verpflichtung der Schüler als Amtsträger nach dem Verpflichtungsgesetz nicht möglich sei.

14.7.4 Hundesteuer

Selbst bei Verwaltungstätigkeiten wie der Erhebung von Hundesteuern entstehen Datenschutzprobleme, die auch Gegenstand der Beurteilung durch die DSK gewesen sind.

So hat sie sich mit der Frage befassen müssen, ob Mitarbeiter einer Verbandsgemeinde, die mit der Ablesung von Wasseruhren beauftragt waren, gleichzeitig auch das Halten von Hunden überprüfen dürfen.

Die DSK hat die Auffassung vertreten, daß den Beauftragten zur Ablesung der Wasserzähler von den Bürgern nur eine zweckgebundene Einwilligung bezüglich des Zutritts in Wohnräume gewährt wird. Diese Einwilligung ist grundsätzlich beschränkt auf das Ablesen der Wasserzähler, der dadurch erreichte Zutritt der gemeindlichen Beauftragten kann nicht zu anderen Zwekken (gleich welcher Art) mitgenutzt werden. Ausnahmen sind nach Auffassung der DSK – wenn überhaupt – nur unter den Voraussetzungen des § 35 StGB (übergesetzlicher Notstand) oder des § 138 StGB (Strafbarkeit der Nichtanzeige geplanter Verbrechen) denkbar. Ein solcher Ausnahmefall war nicht ersichtlich.

Aber auch die Frage, welche Nachweise von Steuerbefreiungstatbeständen vorzulegen sind, welche Kontrollmitteilungen im Hundesteuerbereich an andere Gemeinden gelangen dürfen sowie welche Datenübermittlungen aus der Hundesteuerkartei zum Zweck der Verfolgung privater Rechtsansprüche möglich sind, haben die DSK beschäftigt; sie hat dazu Vorschläge gegenüber dem ISM formuliert, um die veröffentlichte Mustersatzung sowie das Kommunalabgabengesetz in datenschutzrechtlich sinnvoller Weise zu ergänzen. Das ISM hat sich den Vorschlägen der DSK grundsätzlich angeschlossen.

15 Automatisierte Personaldatenverarbeitung und Personalaktenführung

15.1 Vorbemerkung

Im Berichtszeitraum hat sich der Trend fortgesetzt, automatisierte Datenverarbeitungsanlagen, insbesondere Personalcomputer, für Personalverwaltungszwecke einzusetzen. Näheres dazu siehe unter Tz. 15.2.

Die damit zusammenhängenden Fragen haben aus datenschutzrechtlicher Sicht die Notwendigkeit verstärkt, das Personalaktenrecht unter Einschluß der aufgrund der automatisierten Personaldatenverarbeitung zu regelnden Fragen gesetzlich zu normieren. Ein vorliegender Referentenentwurf gibt zu der Hoffnung Anlaß, daß auch in diesem Bereich in nicht allzu ferner Zukunft Fortschritte erzielt werden können (siehe dazu unten Tz. 15.3).

15.2 Automatisierte Personaldatenverarbeitung

Eine größere Zahl von Anmeldungen zum Datenschutzregister hat der DSK einen Überblick über die hier bestehenden Fragen gegeben. Diese Anmeldungen waren Anlaß für Stellungnahmen der DSK aus datenschutzrechtlicher Sicht. Die wichtigsten in diesem Zusammenhang aufgetretenen Probleme sollen im folgenden dargestellt werden.

15.2.1 Datensatz

Zu entscheiden war, ob die Dauer des geleisteten Wehrdienstes gespeichert werden darf, ob Dauer und Grund von Sonderurlauben, Dauer und nähere Angaben zu Krankheiten und insbesondere, ob Prüfungs- oder Examens- und Beurteilungsnoten gespeichert werden dürfen.

Die DSK vertritt die Auffassung, daß nach der bestehenden Rechtslage (§ 23 BDSG, anwendbar gem. § 2 Abs. 3 LDatG) nur die Daten automatisiert gespeichert werden dürfen, die zur Durchführung des öffentlich-rechtlichen Dienstverhältnisses (sei es ein Beamten- oder ein Arbeitsverhältnis) erforderlich sind. Dazu gehören jedenfalls die Dauer des abgeleisteten Wehrdienstes, nicht jedoch alle Noten von Laufbahnprüfungen. Die jeweils letzte Laufbahnprüfung mit Note dürfe ausreichen. Die Speicherung des Krankheitsgrundes ist unzulässig, ein Zusatz, der auf schwangerschaftsbedingte Abwesenheit hindeutet, ist z. B. wegen der regelmäßig in diesen Fällen zu erwartenden längeren Abwesenheit aber erforderlich.

Insbesondere bei der Speicherung von Informationen über Prüfungsabschlüsse und bei Urlaubs- und Krankheitsdaten ist die Frage nach dem Zeitpunkt der Löschung zu problematisieren. Auch in diesen Fällen sind nach der gesetzlichen Regelung die Daten von Amts wegen zu sperren, wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind (§ 25 BDSG). Öffentliche Stellen sollten sich jedoch in diesem Zusammenhang auch an der Löschungsverpflichtung des § 13 LDatG – der für Dienstverhältnisse nicht unmittelbar gilt – orientieren. Danach ist zu löschen, wenn die Informationen zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich sind. Bei Prüfungsnoten dürfte dies dann der Fall sein, wenn zwischenzeitlich etwa zwei Beurteilungsnoten vorliegen. Urlaubsdaten dürften mit endgültiger Abwicklung der Urlaubsansprüche zu löschen sein. Krankheitsdaten sind ebenfalls regelmäßig nach Abschluß des betreffenden Kalenderjahres zu löschen, es sei denn, daß diese Informationen in besonderen Fällen auch künftig bedeutsam sind (etwa bei besonderer Häufigkeit krankheitsbedingter Abwesenheiten).

Die Mitbestimmungsregelung für die Einrichtung von Personalinformationssystemen (§ 77 a Nr. 5 Personalvertretungsgesetz) wurde nicht immer beachtet.

Immer wieder war auch darauf hinzuweisen, daß insbesondere sensiblere Personaldaten (Krankheitsdaten, Qualifikationsdaten) nur strikt zweckgebunden (orientiert am ursprünglichen Speicherungszweck) verwandt werden dürfen und daß dies sowohl durch angemessene Zugriffssicherungen wie durch klarstellende Regelungen etwa auf Ebene von Dienstvereinbarungen oder Dienstanweisungen den Systemnutzern deutlich gemacht werden muß. Zur Zweckbindung von Beihilfedaten siehe unten Tz. 15.4.1.

15.2.2 Zugriffsbefugnisse von Aufsichtsbehörden auf Personalinformationssysteme

Im Berichtszeitraum wurde problematisiert, ob und ggf. in welchem Umfang Aufsichtsbehörden (Ministerien) Zugriff auf die Personaldaten der ihnen nachgeordneten Dienststellen haben dürfen.

Die DSK hat hierzu wie folgt Stellung genommen:

- Soweit Personalentscheidungen delegiert worden sind, d. h. also, soweit die Aufsichtsbehörde nicht unmittelbar mit der Entscheidung von konkreten Personalfragen im Einzelfall befaßt ist, ist ein Direktzugriff der Aufsichtsbehörde auf die Daten der Bediensteten nachgeordneter Stellen nicht erforderlich und damit auch nicht zulässig.

- Für Zwecke der Personalplanung und der damit im Zusammenhang stehenden Statistik ist die Übermittlung anonymisierter Personaldaten ausreichend.

- Weder das Prinzip der Ministerverantwortlichkeit noch Aufsichtsbefugnisse als solche begründen die Erforderlichkeit im datenschutzrechtlichen Sinn zum Zugriff auf alle Bedienstetendaten nachgeordneter Stellen.

Die DSK hat diese Wertung in einer ausführlichen Stellungnahme begründet und auch mit den anderen Mitgliedern der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erörtert.

Die Konferenz hat die Auffassung der DSK unter weitgehender Akzeptierung der von ihr in der genannten Stellungnahme angeführten Gründe bestätigt.

Das betroffene Ministerium hat schließlich ebenfalls die Stellungnahme der DSK akzeptiert. Nach weiteren Erörterungen von Details – die insbesondere die Frage betrafen, in welchem Umfang eine wirkliche Delegation von Personalentscheidungen auf nachgeordnete Stellen erfolgt ist – konnte auch bezüglich der praktischen Verfahrensweise ein Konsens herbeigeführt werden.

15.2.3 Zentralisierte landesweite Personalinformationssysteme

Im 10. Tätigkeitsbericht (Tz. 14.1) wurde das Personalinformationssystem der Oberfinanzdirektion Koblenz dargestellt. Zwischenzeitlich wurde eine ausführliche Dienstanweisung hierzu erlassen, die mehrere Regelungen enthält, die von der DSK ausdrücklich begrüßt worden sind. So ist vorgesehen, daß Personal-Mitteilungen aus dem System an die Betroffenen versandt werden, damit diese die Möglichkeit haben, die Richtigkeit der gespeicherten Daten zu überprüfen. Außerdem wird auf diesem Weg gewährleistet, daß die Betroffenen umfassend informiert werden. Bei Ausdrucken aus dem System erhält das Druckergebnis automatisch den Namen des Benutzers, der den Ausdruck veranlaßt hat. Die Merkmale „Ausbildungsbeurteilungen" und „Prüfungswiederholer" werden nach kurzen Fristen gelöscht. Auch der Grundsatz „keine Eingabe ohne Papierbeleg" ist festgeschrieben worden.

Bei anderen Regelungen war sich die DSK noch nicht sicher, ob damit den datenschutzrechtlichen Belangen ausreichend Rechnung getragen wird. So sind insbesondere die vorgesehenen Auswertungsbeschränkungen, die Zugriffsbeschränkungen sowie die Vertretungsregelungen beim Zugriff auf Datenbestände noch prüfungsbedürftig. In diesem Zusammenhang war die DSK jedoch der Auffassung, daß eine Beurteilung dieser Regelungen erst vor dem Hintergrund praktischer Erfahrungen getroffen werden kann. Sie hat deshalb die OFD Koblenz gebeten, über die gewonnen Erfahrungen nach einer angemessenen Zeit (spätestens nach zwei Jahren, im September 1990) zu berichten.

Auch mit einer anderen zentralisierten Personaldatei hat sich die DSK befaßt: Bei der Staatskanzlei wird herkömmlich eine manuelle Datei derjenigen Bediensteten geführt, deren Ernennungsrecht beim Ministerpräsidenten liegt (§ 13 Landesbeamtengesetz und §§ 1 und 3 der dazu ergangenen Landesverordnung). Früher waren dies alle Bediensteten ab Besoldungsgruppe A 15 bei Beamten sowie BAT I bei Angestellten im Landesdienst. Im Zuge des Einsatzes automatisierter Datenverarbeitung in der Staatskanzlei war beabsichtigt, auch diesen Bereich automationsunterstützt zu bearbeiten. Angesichts der umfassenden, ressortübergreifenden Personaldatei hat die DSK einige Anregungen in diesem Zusammenhang formuliert. Die Staatskanzlei ist dem weitgehend gefolgt. Sie hat darüber hinaus das Ernennungsrecht des Ministerpräsidenten künftig auf Ämter der Besoldungsgruppe ab A 16 (und vergleichbare Angestellte) beschränkt, so daß auch rein quantitativ die Bedeutung dieser Datei erheblich geringer geworden ist.

15.2.4 Automatisierte Telefondatenspeicherung – ISDN –

Im Zusammenhang mit der Einführung der digitalisierten Informationsübermittlung bei der Post (ISDN) werden den Nutzern dieses neuen Übertragungssystems Dienstleistungen angeboten, die auch im Personalbereich datenschutzrechtliche Probleme aufwerfen. So werden künftig grundsätzlich die Teilnehmerinformationen (welcher Anschluß mit welchem Anschluß zu

welcher Zeit wie lange verbunden war) automatisiert gespeichert. Die damit verbundenen Fragen (Schutz des Angerufenen bei Privatgesprächen öffentlich Bediensteter; unbeeinträchtigte Tätigkeit von Personalräten; Schutz der Vertraulichkeit bei besonderen Beratungsdiensten) werden zur Zeit erörtert. Die DSK sieht auch hier jedoch keine unüberwindlichen Probleme für datenschutzgerechte Lösungen.

15.2.5 Leistungsdatenerfassung bei der Nutzung automatisierter Systeme

Die DSK hatte sich auch damit zu befassen, in welchem Umfang Leistungsdaten von Stenotypistinnen erfaßt werden dürfen, die an automatisierten Systemen die Eingabetätigkeit ausüben. Problematisiert wurde diese Frage im Zusammenhang mit Stenotypistinnen der Finanzverwaltung. Die DSK konnte erreichen, daß Auswertungen aus den erfaßten Leistungsdaten künftig nicht mehr ohne konkreten Anlaß und systematisch durchgeführt werden, sondern nur als nichtpersonenbezogene Übersichten und nur zu bestimmten Zwecken.

Die Finanzverwaltung hat auch angekündigt, daß durch den Einsatz neuer Betriebssysteme künftig eine automatische Leistungsdatenerfassung, die auf Finanzamtsebene z. Z. noch technisch unkontrollierbar abgerufen werden kann, nicht mehr möglich sein wird. Die DSK hat auf eine möglichst rasche Einführung der technischen Änderungen gedrängt. Die Finanzverwaltung bezeichnete Ende 1989 als den dafür maßgeblichen Termin.

In diesem Zusammenhang begrüßt die DSK die im Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informationstechnik (vom 30. Mai 1988, Rundschreiben des Ministeriums der Finanzen vom 27. Juli 1988, MinBl. S. 386) getroffene Regelung über Leistungs- und Verhaltenskontrollen. Diese Vorschrift lautet:

§ 9
Leistungs- und Verhaltenskontrollen

(1) Technische Möglichkeiten, mit denen Geräte der Informationstechnik vom Hersteller angeboten werden und die sich zur Kontrolle der Leistung oder des Verhaltens der Bedienungskräfte eignen, die jedoch nicht zur Aufgabenerfüllung vorgesehen werden sollen, werden unbeschadet der Absätze 2 bis 4 nicht genutzt.

(2) Personenbezogene Daten der Bedienungskräfte, die bei der Aufgabenerfüllung anfallen, werden nicht ständig und systematisch zur individuellen Leistungs- oder Verhaltenskontrolle ausgewertet. Über die beabsichtigte Nutzung von Kontrollmöglichkeiten aus konkretem Anlaß anhand solcher personenbezogener Daten sollen die betroffenen Bedienungskräfte vorher informiert werden.

(3) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage mit Hilfe von Geräten der Informationstechnik gespeichert werden, dürfen nicht für Zwecke der individuellen Leistungskontrolle der Bedienungskräfte und zur Kontrolle ihres Verhaltens nur insoweit verwendet werden, als dies zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage erforderlich ist.

(4) Die Einschränkungen für Kontrollmaßnahmen gelten nicht, wenn Tatsachen bekannt werden, die den Verdacht einer Dienstpflichtverletzung rechtfertigen.

15.3 Entwurf eines Gesetzes zur Neuregelung des Personalaktenrechts

Bereits in ihrer Stellungnahme zu den Auswirkungen des Volkszählungsurteils hat die Konferenz der Datenschutzbeauftragten und der DSK Rheinland-Pfalz gefordert, daß datenschutzrechtliche Regelungen für Arbeitsverhältnisse und öffentlich-rechtliche Dienstverhältnisse getroffen werden müssen (Entschließung der Konferenz vom 27. März 1984, Anlage 1 zum 10. Tätigkeitsbericht der DSK).

Nunmehr liegt ein Referentenentwurf des Bundesinnenministeriums zur Neuregelung des Personalaktenrechts vor. Als Anlage 6 ist die dazu formulierte Stellungnahme der DSK abgedruckt, die im wesentlichen gleichlautend mit anderen Datenschutzbeauftragten abgegeben worden ist.

15.4 Einzelfragen zum Personalaktenrecht

15.4.1 Beihilfe

Die DSK hat im Berichtszeitraum gegenüber dem Ministerium der Finanzen die Notwendigkeit betont, Beihilfeangelegenheiten auch organsatorisch so zu behandeln, daß Informationen aus diesem Bereich nicht zu Zwecken der allgemeinen Perso-

nalverwaltung genutzt werden können. Durch die Zentralisierung der Beihilfestellen ist für den größten Teil der Landesbediensteten diese Frage positiv gelöst. Auf Ebene der gemeindlichen Verwaltung sowie bei einigen wenigen Teilen der Landesverwaltung besteht jedoch nach wie vor die problematische Situation, daß Personen für die Beihilfezahlung verantwortlich sind, die gleichzeitig Funktionen im Bereich der allgemeinen Personalsachbearbeitung haben. Ein Versuch der DSK, diese Frage durch eine Ergänzung der Beihilfeordnung zu lösen, war leider nicht erfolgreich. Die DSK geht davon aus, daß die oben (Tz. 15.3) erwähnte gesetzliche Regelung auch dieses Problem zufriedenstellend behandelt.

Die DSK hat im Zusammenhang mit der Beihilfegewährung auch ein anderes Problem aufgegriffen: Ihr ist bekannt geworden, daß Beihilfeanträge, die sich auf Sterilisationen sowie auf Schwangerschaftsunterbrechungen beziehen, ausnahmslos dem FM zur Entscheidung übermittelt werden.

Sie hat in diesem Fall die Frage der Erforderlichkeit einer solchen Verfahrensweise und der Tragfähigkeit der dafür herangezogenen Rechtsgrundlagen gestellt. Die Erörterungen mit dem FM sind zu diesem Punkt noch nicht abgeschlossen.

15.4.2 Verwendungsbeschränkung der Information über Noten der Staatsprüfungen

Im Bereich des Kultusministeriums wurde durch eine Eingabe die Frage problematisiert, ob die Note der Staatsprüfung vom Schulleiter zur Beurteilung der ihm zugewiesenen Lehrer herangezogen werden sollte. Die DSK ist von folgenden Überlegungen ausgegangen: Die Benennung der Staatsprüfungsnoten in der dienstlichen Beurteilung von Lehrern ist für sich genommen kein Eingriff in das informationelle Selbstbestimmungrecht der betroffenen Lehrer. Unter datenschutzrechtlichen Gesichtspunkten relevant ist jedoch, ob die Note der Staatsprüfungen inhaltlich für die Beurteilung eine Rolle spielen sollte. Da das Kultusministerium bereits in der Vergangenheit die Auffassung geäußert hat, daß dies nicht der Fall sein sollte, hat die Gestaltung der Beurteilungsformulare – in denen die Staatsprüfungsnote aufgeführt war – das Mißverständnis nahegelegt, daß diese Note auch für den Inhalt der dienstlichen Beurteilung von Bedeutung ist. Um dieses Mißverständnis zu vermeiden, um also die Zweckverwendung der fraglichen Information auf das beabsichtigte Maß zu beschränken, hat die DSK empfohlen, die entsprechenden Beurteilungsformulare zu ändern und keine Rubrik mehr für die Note der Staatsprüfungen vorzusehen. Dies ist in anderen Bereichen des öffentlichen Dienstes in Rheinland-Pfalz bereits geschehen (z. B. im Finanzbereich).

Das Kultusministerium hat sich diesen Überlegungen angeschlossen und angekündigt, sowohl die Richtlinien für die dienstliche Beurteilung von Lehrern sowie die entsprechenden Beurteilungsformulare in diesem Sinne abzuändern.

16 Datenverarbeitung im kommunalen Bereich

16.1 Datenerhebung für Prüfungszwecke

Gemeindliche Steuereinnahmen sind sparsam und wirtschaftlich zu verwalten. Deshalb wird, wenn Geldleistungen an Vereine oder an die Träger öffentlicher Einrichtungen gewährt werden, intensiv geprüft, ob es mit der Beantragung und der Verwendung seine Richtigkeit hat. Selbstverständlich ist hiergegen auch unter datenschutzrechtlichen Gesichtspunkten im Grundsatz nichts einzuwenden.

In der Wahl ihrer Mittel sind die Kommunen indessen nicht vollständig frei. Sofern für Prüfungszwecke personenbezogene Daten erhoben werden ist zu beachten, daß damit in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Auf die damit verbundene Problematik hat die DSK schon wiederholt hingewiesen (zuletzt in ihrem 10. Tätigkeitsbericht, Tz. 17.3).

Im Berichtszeitraum war es der Kindergarten eines kirchlichen Trägers, der sich in einer Eingabe an die DSK dagegen wandte, daß eine Verbandsgemeindeverwaltung die Gewährung von Personalkostenzuschüssen von der Vorlage von Namenlisten der Kinder abhängig machte. Der Verbandsbürgermeister begründete das Vorlageverlangen mit der Notwendigkeit einer Kostenverteilung auf die Ortsgemeinden unter Zugrundelegung der auf diese entfallenden Kinderzahlen. Er hielt es für erforderlich, die Adressen der Kinder zu Kontrollzwecken mit dem Melderegister abzugleichen. Die Leitung des Kindergartens hingegen sah hierin einen Verstoß gegen datenschutzrechtliche Vorschriften.

Die DSK vertrat in der Stellungnahme gegenüber der Verbandsgemeindeverwaltung die Auffassung, daß keine gesetzliche Verpflichtung der Kindergärten besteht, ihr die Anschriftenlisten zur Verfügung zu stellen. Sofern in den Bewilligungsbescheiden eine Obliegenheit für die Zuschußempfänger begründet wird, entsprechende Listen vorzulegen, muß diese dem Gebot der Verhältnismäßigkeit entsprechen, d. h., es muß eine Abwägung stattfinden zwischen einem eventuell bestehenden Interesse der betroffenenen Eltern an einer Nichtweitergabe von Adreßlisten und den Informationsinteressen der Verbandsgemeindeverwaltung. Von dem Vorliegen berechtigter Geheimhaltungsinteressen der Eltern kann angesichts der Sensibilisierung der Bevölkerung für Fragen des Datenschutzes ausgegangen werden. Das Vorhandensein derartiger Interessen bildet den Hintergrund vieler Eingaben an die DSK. Ebenfalls anzuerkennen ist im Grundsatz aber auch das Interesse der Verbandsgemeindever-

waltung, durch Kontrolle eine fehlerhafte Kostenverteilung auf die Ortsgemeinden auszuschließen. Ein Abwägen der Interessen kann indessen nach Auffassung der DSK nur zu dem Ergebnis führen, daß Überwachungsmaßnahmen, wie die regelmäßige Anforderung von Namenlisten der Kinder sie darstellt, nicht angemessen sind. Unbenommen ist der Verbandsgemeinde die Einzelfallkontrolle. Sie kann mit der Bewilligung von Zuschüssen die Bedingung verbinden, daß Stichprobenüberprüfungen zugelassen werden.

Anders ist die Rechtslage zu beurteilen, wenn es sich um die Förderung von Maßnahmen der außerschulischen Jugendbildung handelt. § 6 des 3. Landesgesetzes zur Ausführung des Gesetzes für Jugendwohlfahrt bestimmt u. a. als Voraussetzung der Förderung, daß der Maßnahmenträger sich verpflichtet, den Teilnehmerkreis offenzulegen sowie Teilnehmerlisten und Nachweise über die Förderungsmittel vorzulegen. Anders als bei dem zuvor dargestellten Fall muß hier der Begründung einer Obliegenheit keine Verhältnismäßigkeitsprüfung der zuschußgewährenden Stelle vorausgehen. Diese wurde im Gesetzgebungsverfahren vorgenommen. Die auf der Rechtsprechung des Bundesverfassungsgerichts beruhende Forderung, daß auch Datenerhebungen bei Obliegenheiten bereichsspezifisch gesetzlich zu regeln sind, ist vorliegend erfüllt.

16.2 Berichterstattung über Gemeinderatssitzungen

Die Information der Bürger über das kommunalpolitische Geschehen ist eine wichtige und förderungswürdige Aufgabe, deren Wahrnehmung freilich auch unter datenschutzrechtlichen Gesichtspunkten von Bedeutung sein kann. Dies ist dann der Fall, wenn über Sachentscheidungen der Gemeindeorgane unter Namensnennung oder in einer Weise berichtet wird die erkennen läßt, auf wen sich diese Entscheidungen beziehen oder wer von ihnen betroffen ist.

So wurde beispielsweise in einer Eingabe an die DSK die Art und Weise gerügt, in der eine Verbandsgemeinde im amtlichen Teil ihres Nachrichtenblattes über die Neuverpachtung einer Jagd berichtete. Der Bericht enthielt die Namen der Pächter sowie genaue Angaben über die jeweils zu entrichtende Jagdpacht und die Wildschadenspauschale. In der Eingabe wurde die Befürchtung geäußert, daß das Bekanntwerden dieser Details nachteilige Auswirkungen im Geschäftsbereich des Betroffenen haben könnte.

In einem anderen Falle machte ein Ortsbürgermeister nach Beratung in der Gemeinderatssitzung öffentlich bekannt, auf wessen Initiative eine Straßenbaumaßnahme durch Verfügung der zuständigen Behörde vorübergehend gestoppt wurde. Man möge sich, so wurde die Berichterstattung abgeschlossen, mit Beschwerden wegen der eingetretenen Verzögerung der Baumaßnahme doch bitte nicht an die Gemeindeverwaltung, sondern an die Initiatoren des Baustopps wenden.

Wie auch bei mehreren anderen Vorgängen, die in diesem Bericht dargestellt sind, ist die Rechtsgrundlage für die Beurteilung der Zulässigkeit solcher Informationsvorgänge das Verwaltungsverfahrensgesetz. Die Beteiligten haben Anspruch darauf, daß ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden (§ 1 Landesverwaltungsverfahrensgesetz i. V. m. § 30 Verwaltungsverfahrensgesetz des Bundes). Diese Bestimmung ist auch bei Berichterstattungen in Wochenzeitungen der Verbandsgemeindeverwaltungen über die Ergebnisse von Gemeinderatssitzungen oder bei der Herausgabe von Presseinformationen zu beachten. Das im Verwaltungsverfahren geltende Geheimhaltungsprinzip zwingt auch dazu, Beratungsgegenstände der geschilderten Art nicht in öffentlichen, sondern in nichtöffentlichen Sitzungen des Gemeinderats – sofern überhaupt dessen Zuständigkeit besteht – zu behandeln. In der Verwaltungsvorschrift zu § 34 Gemeindeordnung sind „Vergabesachen" jedenfalls als Beispiel eines Tagesordnungspunktes der nichtöffentlichen Sitzung genannt. Daß eine öffentliche Berichterstattung über Beratungsdetails nichtöffentlicher Sitzungen nicht in Betracht kommt, sollte selbstverständlich sein.

Das ISM teilt diese Rechtsauffassung der DSK. Die Kommunalreferenten der Bezirksregierungen wurden entsprechend unterrichtet.

Die DSK würde es begrüßen, wenn eine gelegentliche Novellierung der Verwaltungsvorschriften zur Gemeindeordnung für klarstellende Hinweise genutzt würde.

16.3 Rechnereinsatz bei der Kommunalwahl 1989

Schon seit vielen Jahren bedient sich der Landeswahlleiter der automatisierten Datenverarbeitung zur Ermittlung der Ergebnisse von Bundestags- und Landtagswahlen. Nur so ist wohl zu gewährleisten, daß ein vorläufiges amtliches Endergebnis schon wenige Stunden nach Schließung der Wahllokale vorliegt.

Die Feststellung des Ergebnisses von Kommunalwahlen auf örtlicher Ebene war hingegen in der Vergangenheit kein Problem, zu dessen Lösung Computer eingesetzt wurden. Dies lag zum einen daran, daß der Rechenaufwand für die Ergebnisermittlung nach früherem Wahlrecht verhältnismäßig gering war, zum anderen standen bei der vorletzten Kommunalwahl in vielen Städten und fast allen kleineren Gemeinden noch keine Rechner und insbesondere keine geeignete Software zur Verfügung.

Diese Ausgangslage war bei der Kommunalwahl dieses Jahres verändert: Die Wahlrechtsreform 1988 ließ eine weitaus schwierigere Stimmenauszählung erwarten und der Einsatz leistungsfähiger Kleinrechner hatte in den zurückliegenden Jahren eine solche Verbreitung erfahren, daß es durchaus sinnvoll erschien, ihre Nutzung für diesen Zweck zuzulassen.

Die rechtliche Grundlage hierfür wurde durch eine Änderung der Kommunalwahlordnung am 21. September 1988 geschaffen. Es wurde zugelassen, daß die Zählung der Stimmen auch im automatisierten Verfahren erfolgen kann; zugleich wurde bestimmt, daß nur vom Landeswahlleiter freigegebene Programme eingesetzt werden dürfen (§ 53 Abs. 10).

Das damit zugelassene Auszählungsverfahren ist von datenschutzrechtlicher Relevanz, denn es hat die Erfassung und Speicherung der auf die einzelnen Wahlbewerber entfallenden Stimmen zur Voraussetzung und ist damit personenbezogen. Es ist auch nicht gänzlich abwegig, sich vorzustellen, daß die gespeicherten Daten mißbräuchlich verwendet werden könnten. Die fortdauernde Verfügbarkeit der im Speicher der Arbeitsplatzrechner abgebildeten Stimmzettel könnte beispielsweise dazu genutzt werden, Reihungslisten der von den Wählern in den Wahlvorschlägen gestrichenen Bewerber herzustellen. Solche Erkenntnisse könnten, mehr noch als ein schlechtes Wahlergebnis, das schnelle Ende einer politischen Karriere einleiten. So könnten zum Beispiel auch durch unzulässige Datenauswertungen Erkenntnisse über Wahlbewerber gewonnen werden, auf die in der Persönlichkeitswahl Stimmen entfielen, obwohl in der Listenwahl eine andere Partei bevorzugt wurde.

Mit der Anwendung automatisierter Verfahren stellt sich indessen nicht nur die Frage nach dem Persönlichkeitsschutz der Wahlbewerber, sondern, wenn auch nicht unmittelbar zum Zuständigkeitsbereich der DSK gehörend, auch das Problem der Sicherheit und Ordnungsmäßigkeit des Zähl- und Berechnungsverfahrens.

Unmittelbaren Anlaß für Kontrollmaßnahmen der DSK gaben Hinweise aus der Bevölkerung, daß die Gemeinden Geräte aus den verschiedensten Arbeitsbereichen und auch von Firmen und Privatpersonen angemietete Arbeitsplatzrechner für die Auszählung nutzen. Mitglieder von Wahlvorständen beklagten, daß selbst kurze Zeit vor dem Wahltermin noch keine Möglichkeit bestehe, die Arbeitsweise der einzusetzenden Geräte kennenzulernen und die Richtigkeit der Programme zu überprüfen.

Die DSK stellte folgendes fest:

- Die nach § 10 LDatG erforderlichen Anmeldungen zum Datenschutzregister waren fast ausnahmslos unterblieben. Ebenso unterblieb die Verpflichtung der bei der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis nach § 8 LDatG und die Festlegung von Sicherungsmaßnahmen in Dienstanweisungen nach § 9 Abs. 2 LDatG.

- Die freigegebenen Programme waren nicht ausreichend dokumentiert. Ein für den Großrechnereinsatz bestimmtes Programm wurde nicht hinreichend getestet. Dies führte zu fehlerhaften Auszählungsergebnissen und mehrmaliger Wiederholung des Auszählungsvorganges.

- Aufgrund der ungenügenden Programmdokumentation war es den Mitgliedern der Wahlvorstände kaum möglich, die Identität der angewendeten mit den freigegebenen Programmen zu überprüfen.

- Von den Softwareherstellern wurden nach der Programmfreigabe noch Programmänderungen vorgenommen, die ebenfalls nicht dokumentiert waren.

- Es war keine Vorsorge dafür getroffen, daß auf den Festplatten angemieteter Geräte ein genügend großer Speicherplatz für die Datenverarbeitung unter Einsatz der Zählprogramme zur Verfügung stand. Dies führte, wie der DSK später bekannt wurde, in mehreren Fällen zum Abbruch der automatisierten Auszählung.

- Es war auch keine Vorkehrung getroffen, daß die auf Festplatten gespeicherten kandidatenbezogenen Daten vor der Geräterückgabe physisch gelöscht werden. Die DSK sah die Gefahr, daß diese Daten von den Geräteeigentümern für unzulässige Auswertungen weiter genutzt werden könnten.

Die Initiativen der DSK bewirkten, daß der Landeswahlleiter wenige Tage vor dem Wahltermin die Einsatzbedingungen für die von anderen Verwaltungsbereichen oder von Privaten überlassenen Arbeitsplatzrechner konkretisierte. In einem Rundschreiben stellte er klar, daß sie für die Stimmenauszählung nur dann eingesetzt werden dürfen, wenn jegliche unbefugte Datennutzung nach der Stimmenauswertung durch vollständige und endgültige Löschung der Plattenspeicher ausgeschlossen ist. Soweit Angaben auf der Festplatte gespeichert werden, sah er dies nur dann als gewährleistet an, wenn die vollständige Löschung durch ein entsprechendes Programm erfolgt oder wenn auf der Festplatte ausschließlich Daten der Stimmenauswertung gespeichert sind, die nach Fertigung der Niederschrift insgesamt gelöscht werden können.

Bei künftigen Kommunalwahlen sollte der Einsatz von Arbeitsplatzrechnern mit größerer Sorgfalt und unter genauerer Beachtung der gesetzlichen Bestimmungen vorbereitet werden. Eine rechtzeitige Inanspruchnahme ihrer Beratung würde von der DSK begrüßt.

16.4 Kommunale Datenverarbeitung Rheinland-Pfalz GmbH (KDV-GmbH)

Das ISM informierte die DSK im August 1989 über die Absicht, eine Gesellschaft zu gründen, der folgende Aufgaben obliegen sollten:

- DV-technische und -fachliche Beratung der Kommunalverwaltungen,
- Bereitstellung eines umfassenden Angebots (Kommunalpaket) von Verfahren, die sich auf dem neuesten DV-technischen Stand befinden, und in ein Kommunikationskonzept (z. B. Datenfernübertragungsnetz Rheinland-Pfalz) eingebunden sind,
- Sicherstellung der Programmentwicklung und -pflege der dezentral eingesetzten Verfahren,
- Einbeziehung des kommunalen Personals in die DV-Aus- und Fortbildung.

Die DSK nahm zu dem Projekt im wesentlichen wie folgt Stellung:

Bei allen existierenden sogenannten landeseinheitlichen Verfahren stellt sich das Problem der datenschutzrechtlichen Verantwortlichkeit. Normadressaten datenschutzrechtlicher Bestimmung sind in aller Regel die speichernden Stellen; tatsächlich haben diese indessen kaum eine Möglichkeit, die Einhaltung datenschutzrechtlicher Bestimmungen zu gewährleisten. So erfüllen beispielsweise nach § 37 MG die Meldebehörden ihre Aufgaben mit Hilfe des beim Landesrechenzentrum betriebenen und unterhaltenen landeseinheitlichen Verfahrens für das Meldewesen. Die Gemeinden sind von Gesetzes wegen gehalten, sich für die Aufgabenerfüllung eines Verfahrens zu bedienen, auf dessen Gestaltung und Ablauf sie kaum Einfluß nehmen können. Es ist im Prinzip ungeklärt, wie diese Situation unter rechtlichen Gesichtspunkten zu bewerten ist. In der Praxis wurde so verfahren, daß Fragen, die dieses landeseinheitliche Verfahren betrafen, mit dem ISM unmittelbar, bei geringerer Bedeutung auch mit dem Landesrechenzentrum erörtert wurden. Diese Art und Weise der Sachbehandlung führte in aller Regel zu befriedigenden Ergebnissen; die DSK hat deshalb in der Vergangenheit davon abgesehen, die Frage der datenschutzrechtlichen Verantwortlichkeit für landeseinheitliche Verfahren in die rechtliche Beurteilung einzubeziehen.

Mit der Gründung einer privatrechtlich organisierten Gesellschaft, der die Bereitstellung landeseinheitlicher Verfahren und faktisch mindestens die Vorentscheidung über deren Einsatz obliegt, tritt eine wesentliche Änderung dieser Situation ein. Die DSK muß dann datenschutzrechtliche Fragen mit einer Organisation erörtern, deren Handeln außerhalb der Ministerverantwortung liegt.

Ein Teil der im Entwurf des Gesellschaftsvertrages beschriebenen Aufgaben liegt in der Zuständigkeit der speichernden Stellen. Bei diesen kann die DSK beispielsweise auf die Programmentwicklung Einfluß nehmen, indem sie sich über die inhaltliche Gestaltung informiert und Empfehlungen hinsichtlich der Berücksichtigung von Softwaresicherungen ausspricht. Bei einem privatrechtlich organisierten Unternehmen hat die DSK, weil die Bestimmungen des LDatG nicht unmittelbar anzuwenden sind, keine originären Kontrollrechte. Es ist daher von einer Verschlechterung der Einflußmöglichkeiten auf eine datenschutzkonforme Verfahrensgestaltung auszugehen.

Die KDV-GmbH wurde am 24. Oktober 1989 gegründet. Die Bedenken der DSK wurden in der Weise berücksichtigt, daß ihr nach dem Gesellschaftsvertrag ein Prüfungsrecht zusteht. Ferner wurde bestimmt, daß das LDatG auf die Gesellschaft Anwendung findet.

Ob dies ausreicht, um den angesprochenen Bedenken Rechnung zu tragen, kann erst beurteilt werden, wenn Prüfungserfahrungen vorliegen.

17 Liegenschaftskataster

17.1 Zweitkataster der Gemeinden

Im Rahmen der Weiterentwicklung des automatisierten Liegenschaftsbuchs (vgl. 11. Tätigkeitsbericht, Tz. 18.1) wurde im Berichtszeitraum für eine Vielzahl von Gemeinden der direkte Zugriff auf das Liegenschaftskataster durch Online-Anschlüsse eröffnet. Damit wurde die Abgabe von Zweitkatastern in Karteiform an diese Gemeinden entbehrlich.

Der mit dieser technischen Weiterentwicklung zweifellos verbundene Rationalisierungseffekt darf nicht darüber hinwegtäuschen, daß auch mit diesem Verfahren Eingriffe in das Recht auf informationelle Selbstbestimmung verbunden sind, für die eine Rechtsgrundlage z. Z. noch nicht existiert.

Die DSK hat diese durch die Einrichtung von Direktabrufverfahren entstandene Problematik zum Anlaß genommen, die Schaffung normenklarer gesetzlicher Datenerhebungs- und Verarbeitungsbestimmungen für den Katasterbereich zu fordern. Sie hat dabei freilich eingeräumt, daß die Priorität für entsprechende gesetzgeberische Maßnahmen unter dem Gesichtspunkt der Eingriffsschwere im Verhältnis zu anderen Bereichen der öffentlichen Verwaltung – jedenfalls im Blick auf den gegenwärtigen Umfang der Datenspeicherung – nicht allzu hoch anzusetzen ist.

Das ISM hat die Forderungen im Grundsatz anerkannt. Es hält insbesondere die Vorschriften über den Zweck des Liegenschaftskatasters sowie die Regelungen über die Verpflichtung der Betroffenen zur Abgabe grundstücks- und personenbezogener Daten und die Bestimmungen über die Benutzung des Liegenschaftskatasters für präzisierungsbedürftig. In jüngster Zeit fand eine erste Erörterung von Regelungskonzepten unter Beteiligung eines Vertreters der DSK statt.

17.2 ALB als fachübergreifendes Informationssystem

Auch die Weiterentwicklung des Liegenschaftskatasters mit dem Ziel der Schaffung eines fachübergreifenden Informationssystems kommt voran. Mit dem aktuellen Nachweis der tatsächlichen Nutzung des Grund und Bodens und von Ergebnissen der Bodenschätzung enthält es bereits jetzt Basisdaten, die für Zwecke des Umwelt- und Bodenschutzes benötigt werden. Außerdem werden alle Flurstücke, die in Natur-, Wasser-, Heilquellen- und Grabungsschutzgebieten sowie in Abfalldeponien liegen, im Liegenschaftskataster durch entsprechende Hinweise gekennzeichnet.

In diese Entwicklung eingebunden ist auch die Funktionserweiterung des Liegenschaftskatasters als lagebezogenes Rebflächenverzeichnis und dessen Verbindung mit der betriebsbezogenen Weinbaukartei. Rechtsgrundlagen hierfür sind die Verordnung (EWG) Nr. 649/87 der Kommission vom 3. März 1987 (ABl. EG Nr. L 62 S. 10), § 1 der Vierten Landesverordnung zur Durchführung des Weinwirtschaftsgesetzes vom 17. August 1984, GVBl. S. 187, BS 7821-22, sowie die Verwaltungsvorschrift vom 1. August 1989, MinBl. S. 292.

Die Datenbasis für diese Funktionserweiterung wird gebildet durch

- den Nachweis der Weinlagen (Weinlagenverschlüsselung),

- Hinweise bei den Flurstücken, für die eine weinbauliche Nutzung nicht mehr gestattet ist sowie

- Hinweise bei den Flurstücken, die innerhalb der zur Erhaltung des Steillagenweinbaues abgegrenzten Gebiete liegen.

Auch diese Entwicklungen unterstreichen die von der DSK erhobenen Forderungen nach einer klaren Aufgabenbeschreibung des Liegenschaftskatasters sowie nach gesetzlichen Regelungen für die Datenerhebung und -verarbeitung, die den Anforderungen des Bundesverfassungsgerichts im VZU entsprechen.

17.3 Befragung zur Gewinnung von Zusatzinformationen für die Kaufpreissammlung

Aufgrund der Bestimmungen des Baugesetzbuchs (§§ 192 ff.) und der hierzu ergangenen Gutachterausschußverordnung sind in den kreisfreien und großen kreisangehörigen Städten sowie in den Landkreisen Gutachterausschüsse eingerichtet. Diese sind als selbständige und unabhängige Kollegialorgane zuständig für die Ermittlung von Grundstücks- und Gebäudewerten. Die Datenbasis für die Wahrnehmung dieser Aufgaben bildet die Kaufpreissammlung, in die nach Auswertung die wertbeeinflussenden Merkmale aus Grundstücksverträgen übernommen werden. Durch § 195 Baugesetzbuch sind die beurkundenden Stellen gehalten, Verträge, durch die sich jemand verpflichtet, Eigentum an einem Grundstück gegen Entgelt, auch im Wege des Tausches, zu übertragen oder ein Erbbaurecht zu begründen, in Abschrift dem Gutachterausschuß zu übersenden.

Da der Grundstücksmarkt jedoch auch von Umständen und Wertmerkmalen beeinflußt wird, die aus den Kaufverträgen in der Regel nicht hervorgehen, führen die Geschäftsstellen der Gutachterausschüsse eine Zusatzbefragung auf freiwilliger Grundlage durch. Die formalen Anforderungen des § 5 Abs. 2 und 3 Landesdatenschutzgesetz sind hierbei erfüllt: Die Betroffenen werden darauf hingewiesen, daß die Mitwirkung bei der Erhebung freiwillig ist, aus einer Nichtbeantwortung der Fragen keine Nachteile entstehen, und daß der Inhalt der Vertragsabschriften und die gewonnenen Daten vertraulich behandelt werden. Durch die Einwilligungserklärung nicht gedeckt ist indessen die Übermittlung der Daten. Eine solche Übermittlung läge vor, wenn der Inhalt der Kaufpreiskartei aufgrund gesetzlicher Vorschriften an das zuständige Finanzamt weitergegeben (§ 195 Abs. 2 und 3 Baugesetzbuch) oder wenn aus der Kaufpreiskartei Auskünfte erteilt werden (§ 15 Gutachterausschußverordnung). Wer beispielsweise im Rahmen der Zusatzbefragung freiwillig die Frage nach der Monatsmiete einer Wohnung beantwortet, muß auch wissen, daß diese Angaben als wertbeeinflussende Umstände (Ertrag baulicher Anlagen, § 12 Gutachterausschußverordnung) in der Kaufpreissammlung festgehalten werden kann, und daß diese an das Finanzamt weitergegeben wird, wo sie für Zwecke der Wertermittlung, möglicherweise aber auch für Prüfungszwecke genutzt wird.

Die DSK wies das ISM auf diese Problematik hin. Sie hielt es für erforderlich, entweder auch die Zustimmung zur Datenübermittlung einzuholen oder aber die im Rahmen der Zusatzbefragung erhobenen Daten außerhalb der Kaufpreissammlung zu speichern und nur für interne Zwecke zu nutzen.

Das ISM ordnete daraufhin an, daß die Daten nur für interne Zwecke verwendet werden. Durch organisatorische Maßnahmen wird sichergestellt, daß die im Rahmen der Bürgerbefragung erhobenen Daten in einer ergänzenden Datensammlung gespeichert werden.

17.4 Gutachterausschußverordnung

Die Erteilung von Auskünften aus den Kaufpreissammlungen ist als datenschutzrechtliches Problem schon sehr lange in der Diskussion. Aufgrund der vorläufigen Richtlinien des ISM für die Einrichtung und Führung von Kaufpreissammlungen vom 24. August 1979 war zugelassen, daß auf Antrag Auskünfte aus den Kaufpreissammlungen an Stellen innerhalb des öffentlichen Bereichs gegeben werden, wenn die Auskünfte zur rechtmäßigen Aufgabenerfüllung erforderlich sind. Ferner war bestimmt, daß in gleicher Weise bei entsprechenden Anträgen von öffentlich bestellten und vereidigten Sachverständigen zu verfahren ist, wenn sich diese verpflichten, nur die unbedingt erforderlichen personenbezogenen Daten zu entnehmen, in Gutachten usw. nur anonymisierte Daten aufzunehmen und nach Auswertung der personenbezogenen Daten diese zum frühestmöglichen Zeitpunkt zu löschen.

Die DSK hatte in ihrem 7. Tätigkeitsbericht (Tz. 8.7) Zweifel geäußert, ob diese Richtlinien in vollem Umfange mit den Übermittlungsbestimmungen des Landesdatenschutzgesetzes in Übereinstimmung stehen; weil das ISM indessen immer wieder die zwingende Notwendigkeit einer Bekanntgabe personenbezogener Daten an Sachverständige betonte, wurde die Regelung toleriert.

Eine Änderung der rechtlichen Ausgangslage ist durch die Novellierung des Bundesbaugesetzes eingetreten. Durch § 199 Abs. 2 Baugesetzbuch ist die Landesregierung nunmehr ermächtigt, die erforderlichen Auskunftsregelungen durch Rechtsverordnung zu schaffen. Dies ist inzwischen geschehen: Durch § 15 der Gutachterausschußverordnung vom 15. Mai 1989 (GVBl. S. 153) wurde zugelassen, daß Behörden und sonstigen öffentlichen Stellen sowie den öffentlich bestellten und vereidigten Sachverständigen im Einzelfall Auskünfte aus der Kaufpreissammlung erteilt werden, wenn ein berechtigtes Interesse dargelegt wird und die sachgerechte Verwendung der Daten gewährleistet erscheint. Die Auskünfte dürfen jedoch nur grundstücksbezogen erteilt werden; die Mitteilung des Namens und der Anschrift des Eigentümers oder sonstiger berechtigter Personen ist nicht zugelassen. Anderen Stellen und Personen dürfen nur solche Auskünfte erteilt werden, die Rückschlüsse auf den Eigentümer nicht ermöglichen.

Die DSK stimmte diesen Regelungen, die sie für praxisgerecht hält, zu. Ihren Empfehlungen zur inhaltlichen Gestaltung der Ausführungsbestimmungen wurde entsprochen.

18 Statistik

18.1 Volkszählung 1987

18.1.1 Allgemeines

In Ausführung eines Landtagsbeschlusses berichtete die DSK im April 1987 (Drucksache 10/3163) und im März 1988 (Drucksache 11/1029) über den Ablauf der Volkszählung 1987 und ihre Kontrollarbeit. Der Bericht vom März 1988 wurde auf Antrag der Fraktion der CDU zusammen mit dem 11. Tätigkeitsbericht der DSK in der 30. Sitzung des Landtags Rheinland-Pfalz am 24. Juni 1988 besprochen (Plenarprotokoll S. 2154 ff.).

Eine Landtagsfraktion bemängelte, den Kontrollarbeiten bei den Volkszählungs-Erhebungsstellen habe kein systematisch ausgearbeiteter Prüfungsplan zugrunde gelegen und die Durchführung der Kontrollen sei nicht nach einem einheitlichen Konzept erfolgt. Demgegenüber ist zu betonen, daß sich die Kontrolltätigkeit keineswegs in der Nachprüfung von Eingaben oder in der Reaktion auf Hinweise aus der Bevölkerung erschöpfte. Die DSK hat bei der Festlegung des Prüfungsplans auf die größenmäßige und regionale Verteilung der Erhebungsstellen geachtet und selbstverständlich gingen die Mitarbeiter der DSK-Geschäftsstelle bei örtlichen Prüfungen nach einem im Grundsatz feststehenden, jedoch nach dem jeweiligen Stand des Verfahrens modifizierten Prüfungsschema vor. Daß Erhebungsstellen, deren Arbeit Gegenstand von Eingaben oder Hinweisen an die DSK war, bei der Bestimmung der zu prüfenden Stellen vorrangig berücksichtigt wurden, war angesichts der personellen Ausstattung der DSK-Geschäftsstelle eine zwingende Notwendigkeit.

18.1.2 Bearbeitung und Vernichtung der Erhebungsunterlagen

Im letzten Absatz des oben zitierten 2. Berichts zur Volkszählung 1987 wies die DSK darauf hin, daß die Datenerfassung und -auswertung beim Statistischen Landesamt, die Vernichtung und Löschung von Erhebungsmaterialen und Daten auf Datenträgern sowie die Übermittlung und Verwendung anonymisierter Einzelangaben in den öffentlichen Verwaltungseinheiten Schwerpunkte der weiteren Prüfungstätigkeit bildeten.

Die räumlichen, organisatorischen, personellen und technischen Maßnahmen der Datensicherheit sowie die Bearbeitung von Erhebungsunterlagen wurden in mehreren Kontrollbesuchen beim Statistischen Landesamt überprüft. Das Amt hatte – beraten durch Fachkräfte des Landeskriminalamtes – Maßnahmen getroffen, die der Empfindlichkeit der zu verarbeitenden Materialien entsprachen. Beanstandungen waren nicht auszusprechen.

Die Vernichtung der Erhebungsunterlagen begann am 18. Dezember 1988 und war am 24. Februar 1989 abgeschlossen. Die Notwendigkeit, Erhebungsunterlagen zum Nachweis der Richtigkeit von Zählungsergebnissen in gerichtlichen Auseinandersetzungen mit Städten und Gemeinden aufzubewahren, bestand nicht. Mit der Vernichtung der Materialien war ein Unternehmen beauftragt, das auf derartige Arbeiten spezialisiert ist. Das Unternehmen wurde unangemeldet aufgesucht und kontrolliert. Mängel wurden nicht festgestellt.

18.1.3 Automatisierte Verarbeitung von Volkszählungsdaten beim Statistischen Landesamt

§ 15 Abs. 2 des Volkszählungsgesetzes bestimmt, daß die laufenden Nummern und die Ordnungsnummern der Erhebungsmaterialen durch verfremdete Ziffern, die nur die statistischen Zusammenhänge festhalten, zu ersetzen sind. Dieses Verfahren dient der Reduzierung des Deanonymisierungsrisikos, eine vollständige Anonymisierung wird auf diese Weise indessen nicht erreicht. Eine von den Datenschutzkontrollinstitutionen eingesetzte Arbeitsgruppe erarbeitete Anforderungen an das von den Statistischen Ämtern für die automatisierte Verfremdung zu entwickelnde Programm. Das Statistische Landesamt entsprach diesen Anforderungen.

Für ausschließlich statistische Aufgaben dürfen den zur Durchführung statistischer Aufgaben zuständigen kommunalen Stellen Einzelangaben für ihren Zuständigkeitsbereich auf Datenträgern übermittelt werden, wenn durch Landesgesetz eine Trennung dieser Stellen von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist. Nachdem mehrere größere Städte den hiernach und nach den Vorschriften des Landesstatistikgesetzes zu stellenden Anforderungen (vgl. Tz. 18.2) entsprochen haben, konnte deren Wunsch nach Datenübermittlung ab Juni dieses Jahres entsprochen werden. Eine Prüfung der Datenverarbeitung bei diesen Städten ist vorgesehen.

18.2 Abschottung kommunaler Statistikstellen

§ 14 Abs. 1 des Volkszählungsgesetzes bestimmt, daß den zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände Einzelangaben übermittelt werden dürfen, wenn durch Landesgesetz eine Trennung dieser Stellen von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist. Die gleichen Voraussetzungen bestehen nach § 16 Abs. 5 Bundesstatistikgesetz auch für die Übermittlung von Einzelangaben aus anderen Bundesstatistiken.

Aufgrund dieser Anforderungen und als Voraussetzung für die Übernahme von Einzelangaben aus Landesstatistiken und für die Durchführung von Kommunalstatistiken fordert § 8 Abs. 4 i. V. m. § 5 Abs. 2 des Landesstatistikgesetzes, daß die zuständigen Stellen räumlich, organisatorisch und personell von anderen, mit Aufgaben des Verwaltungsvollzugs befaßten Stellen zu trennen sind.

Im September 1988 fragte die DSK bei den kreisfreien und großen kreisangehörigen Städten des Landes an, in welcher Weise den gesetzlichen Anforderungen an die Abschottung von Statistikstellen entsprochen werde. Aus einem Großteil der Antworten war zu entnehmen, daß konkrete Vorstellungen noch nicht bestehen und daß Beratung durch die DSK bezüglich der gesetzlichen Anforderungen an die Abschottung erwünscht ist.

Die DSK hat in Wahrnehmung ihrer Beratungsfunktion nach § 17 Abs. 1 LDatG die aus ihrer Sicht zu stellenden Anforderungen in einem Katalog zusammengefaßt, der diesem Bericht als Anlage 7 angefügt ist. Der Städtetag Rheinland-Pfalz hat den Anforderungskatalog am 25. April 1989 seinen Mitgliedsstädten übermittelt.

18.3 Hochschulstatistik

Die Bundesstatistik für das Hochschulwesen wird noch immer auf der Grundlage des Hochschulstatistikgesetzes i. d. F. vom 21. April 1980 durchgeführt. Dieses Gesetz ist dringend novellierungsbedürftig, denn es entspricht nicht den verfassungsrechtlichen Grundsätzen, die sich aus dem Volkszählungsurteil des Bundesverfassungsgerichts ergeben.

Die Bundesregierung hat am 11. August 1989 einen Gesetzentwurf eingebracht (Bundesratsdrucksache 416/89), der am 22. September 1989 an die Ausschüsse überwiesen wurde. Durch Umstellung der Erhebungsverfahren, durch Verzicht auf eine personenbezogene Zusammenführung der Studentendaten, durch Wegfall der in der Vergangenheit zugelassenen verwaltungsinternen Verwendungsmöglichkeiten der personenbezogenen Daten und durch Wegfall der Abiturientenbefragung soll sowohl den verfassungsmäßigen Anforderungen als auch der Statistikbereinigung entsprochen werden.

Das im Grundsatz datenschutzfreundliche Bild, das der Entwurf vermittelt, darf nicht darüber hinwegtäuschen, daß das „verbesserte" Erhebungsprogramm auf einer Erweiterung des Erhebungskatalogs beruht. Angesichts des Verzichts auf die Studienverlaufsstatistik mag dies gerechtfertigt sein; bedenklich wäre es freilich, wenn die Bestrebungen einiger Länder, die Studienverlaufsstatistik erneut in das Gesetz einzufügen, erfolgreich wären.

Aus gegebener Veranlassung hat die DSK im Berichtszeitraum die Datenerhebungsvordrucke überprüft, die aufgrund des noch geltenden Hochschulstatistikgesetzes verwendet werden. Sie traf folgende Feststellungen:

- Es ist unzulässig, daß in den Erhebungsvordrucken Verwaltungszwecke und Statistikzwecke nicht deutlich getrennt werden. Es ist irreführend, daß der Erhebungsvordruck mit „Antrag auf Einschreibung/Rückmeldung" überschrieben ist, als Rechtsgrundlage aber ausschließlich Statistikvorschriften genannt werden. Den Auskunftspflichtigen muß verdeutlicht werden, welche Daten für Statistikzwecke auf der Grundlage des Hochschulstatistikgesetzes und welche Daten auf der Rechtsgrundlage des Hochschulgesetzes/Fachhochschulgesetzes und der jeweiligen Einschreibeordnung erhoben werden.

- Einzelne Fragen, die der Datenerhebung für Verwaltungszwecke dienten, befanden sich auf einem Vordruck, der von der Hochschulverwaltung an das Statistische Landesamt weitergegeben wurde. Da die erhobenen Daten für statistische Zwecke nicht erforderlich sind, muß eine Datenübermittlung an das Statistische Landesamt durch verfahrenstechnische Vorkehrungen ausgeschlossen werden.

- Für die freiwillige Beantwortung einzelner Fragen wurde ein Einlageblatt verwendet, das nicht an das Statistische Landesamt weitergegeben wurde, sondern bei der Hochschule verblieb. Am Schluß des Fragebogens hatte der Betroffene unterschriftlich zu bestätigen, daß ihm bekannt ist, daß in dem Antrag gemachte wahrheitswidrige Angaben den Widerruf der Einschreibung zur Folge haben können. Die DSK stellte in Zweifel, ob tatsächlich eine unrichtige, jedoch ohne Verpflichtung erteilte Auskunft eine derart schwerwiegende Rechtsfolge haben könnte.

Das Statistische Landesamt erkannte die Berechtigung der auf diesen Feststellungen beruhenden Forderungen der DSK an. Die Erhebungsvordrucke wurden entsprechend geändert.

18.4 Entwurf einer EG-Statistikverordnung

Die nationalen Statistikämter sollen nach dem Vorschlag der EG-Kommission durch eine Verordnung des Rates der Europäischen Gemeinschaften die Befugnis erhalten, vertrauliche statistische Daten dem Statistischen Amt der Europäischen Gemeinschaften auch dann zu übermitteln, wenn sie einen Personenbezug aufweisen. Es ist nicht auszuschließen, daß auf nationaler Ebene kurzfristig für bestimmte statistische Zwecke vorgehaltene personenbezogene Datenbestände (z. B. noch nicht anonymisierte Daten aus dem Mikrozensus) durch das Statistische Amt der EG abgerufen werden.

Deshalb muß in der EG-Verordnung festgelegt werden, daß die Übermittlung personenbezogener Einzelangaben nur ausnahmsweise durch einen weiteren Rechtsakt der EG für bestimmte statistische Zwecke (z. B. für die Produktions-, Industrie- und Außenhandelsstatistik) zugelassen werden darf und daß eine möglichst frühzeitige Anonymisierung stattfindet sowie notwendige organisatorisch-technische Maßnahmen der Datensicherung getroffen werden.

Die unabhängige Datenschutzkontrolle auf Gemeinschaftsebene ist bisher nicht gewährleistet. Der geplante Beratende Ausschuß kann diese Kontrolle nicht ersetzen.

Im Gemeinschaftsrecht sind bisher für die Verletzung des Statistikgeheimnisses keine ausreichenden Sanktionen vorgesehen. Ein derartiger Verstoß ist nicht einmal in allen Mitgliedsstaaten unter Strafe gestellt.

Die Teilnehmer der 11. Internationalen Konferenz der Datenschutzbeauftragten in Berlin haben am 30. August 1989 diesen Fragenkreis diskutiert und sind übereingekommen, sich auf nationaler und internationaler Ebene für eine stärkere Berücksichtigung datenschutzrechtlicher Belange im Verordnungsentwurf einzusetzen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat unter Beteiligung der DSK am 26./27. Oktober 1989 in diesem Sinne eine Entschließung gefaßt.

Das ISM wurde von der DSK bereits im Juni dieses Jahres über die datenschutzrechtliche Beurteilung des Entwurfs unterrichtet und gebeten, bei den anstehenden Beratungen im Bundesrat auf eine Verbesserung des Datenschutzes hinzuwirken.

19 Technischer und organisatorischer Datenschutz

19.1 Allgemeines

Die Bedeutung der automatisierten Datenverarbeitung und ihr Einsatz am Arbeitsplatz nimmt auch in der öffentlichen Verwaltung stetig zu. Alle Prognosen deuten darauf hin, daß sich die rasante Entwicklung der Computertechnik und des Computereinsatzes in den nächsten Jahren noch beschleunigen wird. Kennzeichen dieser Entwicklung sind die einfachere Handhabung, die verbesserte Kompatibilität, bessere und schnellere Übertragungstechniken und ein stetig verbessertes Preis-Leistungsverhältnis.

Der technische Datenschutz von Arbeitsplatzrechnern war bis vor wenigen Jahren noch von dieser Entwicklung abgekoppelt. Dies hatte zur Folge, daß sensible Anwendungen, wie beispielsweise die Verarbeitung medizinischer Daten oder von Sozialdaten, nicht entsprechend den Bedingungen des Datenschutzgesetzes durchgeführt werden konnten, weil angemessene technische Datensicherungsmaßnahmen nicht zu realisieren waren.

Im Berichtszeitraum hat sich diese Situation grundlegend geändert. Es stehen heute leistungsfähige Hardware- und Softwareprodukte zur Verfügung, die die Sicherheit und den Datenschutz beim Einsatz von Arbeitsplatzrechnern verbessern. Noch sind nicht alle Datensicherungsprobleme gelöst, aber die Zielrichtung ist deutlich: Es geht darum, ein Maß an Datensicherheit zu erreichen, das dem von Großrechnern angenähert ist. Das Kernproblem ist freilich organisatorischer Art und nur durch organisatorische Maßnahmen lösbar. Datensicherungsmaßnahmen werden nicht von den Herstellern der Arbeitsplatzrechner realisiert, sondern sind benutzerseitig zu implementieren. Es ist deshalb wichtig, das Risiko einer Umgehung von Sicherungsmaßnahmen dadurch zu minimieren, daß bei dieser Implementierung auf eine strikte Funktionstrennung der Benutzer geachtet wird. Datensicherungsmaßnahmen sind wenig sinnvoll, wenn ein PC-Anwender beispielsweise in der Lage ist, sie unbemerkt zu umgehen.

Die DSK fordert den Einsatz von Datensicherungsprodukten stets dann, wenn sensible Daten verarbeitet werden sollen und auf andere Weise ein angemessener Datenschutz nicht zu erreichen ist. Die entstehenden Zusatzkosten müssen in Kauf genommen werden und es ist jeder Behörde anzuraten, sie bereits bei der Entscheidung über die Anschaffung von Geräten zu berücksichtigen.

Es sollte dabei beachtet werden, daß eine Datensicherung durch derartige technische Verfahren Leistungsmerkmale bietet, die auch außerhalb von Datenschutzüberlegungen wichtig sind. Sie ist grundsätzlich geeignet, beispielsweise die zweckwidrige Verwendung von Arbeitsplatzrechnern oder das Einschleppen von Computerviren durch Verwendung nicht autorisierter Software zu verhindern. Die Vermeidung eines einzigen Störfalles erspart in der Regel mehr Mittel, als die Anschaffung kostet.

19.2 Personalcomputer (PC)

Aufgrund der relativ niedrigen – und noch stetig weiter fallenden – Anschaffungspreise für Hardware und Software gehört der PC heute mittlerweile zum Standard der Büroausstattung.

Ursprünglich als stand-alone System konzipiert, wird der PC immer häufiger in Netzwerken und als Host-Terminal betrieben. Er hat damit seine frühere Zweckbestimmung, die Benutzer in die Lage zu versetzen, unabhängig von Zentralrechnern Informationen zu speichern, zu bearbeiten oder Daten zu übermitteln, stark erweitert. Heute verfügen PC über die Leistungsfähigkeit (z. B. 80 386 Prozessoren, Direktzugriffsspeicher über 300 MB oder optische Bildplatten) von Großrechnern der 70er Jahre. Die Anwendungsbreite rechtfertigt es, nicht mehr von einem „persönlichen Computer" (PC), sondern von einem „Arbeitsplatzrechner" zu sprechen.

Als Schwachpunkte der Datensicherheit bei Arbeitsplatzrechnern sind zu nennen:

- Fehlender Benutzer- und Paßwortschutz
- Fehlende Beschränkung der Zugriffsmöglichkeiten auf die für die Aufgabenerfüllung erforderlichen Daten
- Keine Funktionstrennung zwischen Sachbearbeiter und Datenverarbeitung
- Das Vieraugenprinzip entfällt.
  Der Bediener kann Sachbearbeiter, Operator, Ausführender der Verarbeitung, Datenträgerverwalter und evtl. Programmersteller in einer Person sein.
- Fehlende Protokollierungsmöglichkeiten
- Zweckentfremden von Programmen und Daten durch Verwendung von Kopien

- Änderung der Hardware (z. B. Adapterkarten), so daß zusätzliche Funktionen und Anschlüsse an andere Systeme möglich sind
- Wartung der Geräte durch Fremdpersonal und außer Haus
- Gefahren durch Fremdprogramme und selbstentwickelte Programme, die nicht freigegeben sind bzw. nicht oder nur mangelhaft dokumentiert sind
- unzureichende Zugangskontrollen.

Überdies muß sich der Anwender beim PC-Einsatz – anders als bei der zentralen Datenverarbeitung – selbst umfassend um die Belange des Datenschutzes und der Datensicherheit kümmern.

Im Blick auf diese Problematik hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der DSK Rheinland-Pfalz am 10. Oktober 1988 einen Beschluß über die Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen gefaßt und gefordert:

- Vor jeder Entscheidung über den Einsatz eines PC oder einer kleinen DV-Anlage muß geprüft werden, ob die erzielbare Datensicherheit ausreichend ist. Die Verarbeitung personenbezogener Daten in einem automatisierten Verfahren, das keine ausreichende Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.

- Eine speichernde Stelle hat bei der Verarbeitung personenbezogener Daten mit Hilfe von PC oder sonstigen kleinen DV-Anlagen geeignete technische und organisatorische Maßnahmen zu treffen, die die Datensicherheit gewährleisten. Soweit dies mit den verfügbaren Mitteln nicht im erforderlichen Umfang erreicht werden kann, muß auf den Einsatz von PC oder kleinen DV-Anlagen verzichtet werden.

- Die Hersteller von Hard- und Software werden aufgefordert für kleine DV-Anlagen einschließlich PC Verfahren zu entwikkeln und bereitzustellen, die beim Betrieb dieser Geräte ein Maß an Datensicherheit ermöglichen, das dem großer Rechenzentren entspricht.

19.3 Datensicherungssoftware und Hardware

Gab es vor einigen Jahren, als die ersten PC zum Einsatz kamen, kaum ausreichende Unterstützung zur Lösung des Sicherheitsproblems, so existieren heute Produkte, die eine deutlich verbesserte Sicherheit bieten.

Sicherheitsprodukte für PC können in 3 Kategorien eingeteilt werden.

- Reine Softwarelösungen

  Hier wird beim Starten des Rechners ein auf der Festplatte vorhandenes Sicherungsprogramm ausgeführt, das durch Paßwortabfrage den Zugang zum Rechner und zu festgelegten Anwendungen steuert. Die Schwachstellen bei reinen Softwarelösungen liegen darin, daß es möglich ist, Programme (z. B. Betriebssystem) von angeschlossenen Diskettenlaufwerken zu starten und damit die Paßwortsicherung zu umgehen.

- Softwarelösungen mit Hardwareunterstützung (Steckkarten)

  Um die Schwächen reiner Softwarelösungen zu umgehen, wird der Softwareschutz mit dem Einbau von Hardwarekarten kombiniert, die die Inbetriebnahme des Rechners von einem Diskettenlaufwerk verhindern und Paßworte oder Verschlüsselungsalgorithmen auf der Karte ablegen.

- Sicherheitssysteme mit spezieller Sicherheitshardware

  Einen hohen Sicherheitsstandard erreichen Hardwaresicherungssysteme, die über einen eigenen Prozessor verfügen. Diese bieten technisch die Möglichkeit, eine Benutzeridentifizierung vor der Ausführung von ladbaren Programmen durchzuführen, d. h. die Entscheidung, wer berechtigter Benutzer ist und welche Befugnisse er hat, wird in der Sicherheitshardware gefällt.
  Bei Sicherheitssystemen, die auf Hardware basieren, muß geprüft werden, inwieweit der Schutz durch Entfernung der Hardwaresicherungen wieder aufgehoben werden kann.

Die zur Zeit auf dem Markt befindlichen Produkte haben im wesentlichen folgende Eigenschaften:

- Die Inbetriebnahme eines Systems ist nur mit Paßwort oder einer ID-Karte möglich

- Vom System erzwungener Paßwortwechsel in bestimmten Zeitintervallen

- Paßwortbildung nach bestimmten Regeln (Mindestzeichenzahl, bestimmte Zeichen, neues Paßwort muß von vorhergehenden abweichen)

- Funktionstrennung zwischen Systembetreuer und Anwender

- Zugang zu Anwendungen (PC, Netzwerk, Host-Verbindung) nur über benutzerindividuelle Menüsteuerung und/oder Paßwörter

- Abgestufte benutzerindividuelle Zugriffsberechtigung (lesen, verändern, löschen)

- Benutzerindividuelle Auswahl der zur Verfügung stehenden Dateien und Verzeichnisse

- Vergabe von Speicherplatzgrenzen je Anwender auf Festplatten

- Benutzerindividuelle Sperrmöglichkeiten des Zugriffs auf das Betriebssystem bzw. einzelne Betriebssystembefehle (z. B. Kopieren, Löschen, Umbenennen usw.)

- Keine Umgehung des Zugriffsschutzes durch Laden des Betriebssystems oder Programme über ein Diskettenlaufwerk (Bootschutz)

- Verschlüsselung sensibler Daten (einzelne Datenbestände, gesamter Datenträger)

- Protokollierung folgender Systemaktivitäten der Systemadministratoren und aller übrigen Benutzer:

  Systemstarts (Logon/Logoff)
  Benutzeranmeldungen (auch Fehlversuche)
  Zugriff auf Dateien, Dateifelder, Programme
  Veränderungen am Schutzsystem
  Kopieren auf Datenträger
  Übermittlungen.

Die DSK hat in der Vergangenheit in verschiedenen Anwendungsbereichen den Einsatz entsprechender Sicherungssoft- und Hardware für die Verarbeitung personenbezogener Daten auf PC gefordert.
Das gilt beispielsweise für die Anwendung von PC im Polizeibereich, bei Staatsanwaltschaften, Betriebsprüfern in Finanzämtern und Laptops von Ärzten der Gesundheitsämter (vgl. Tz. 9.4).

Vor der Entscheidung für den Einsatz eines bestimmten Produktes, ist es erforderlich, eine Sicherheitsanalyse, die sich an den technischen und organisatorischen Gegebenheiten der einzelnen Installationen und Anwendungen (z. B. Standort, bauliche Maßnahmen, Sensivität der Daten, Nutzung der Geräte in Netzwerken oder mit einer Hostverbindung) orientiert, durchzuführen.

Mit dem Einsatz solcher Produkte können nicht alle Risiken beim Einsatz von PC ausgeschaltet werden.
Nur in Fällen, in denen gewährleistet ist,

- daß die mit dem PC zu erledigenden Aufgaben (Funktionstrennung) eng umgrenzt sind,

- nur bestimmte Anwendungsprogramme über Menüsteuerung aufgerufen werden können (d. h. daß keine Universalprogramme wie z. B. dBase, Framework verwendet werden),

- eine sichere Regelung für den Umgang mit Datenträgern existiert (Verschlüsselung),

- und der ordnungsgemäße Gebrauch der Sicherungsmechanismen durch organisatorische Maßnahmen unterstützt und kontrolliert wird,

ist eine Verarbeitung von sensiblen personenbezogen Daten auf PC akzeptabel.

Weiterhin ist es wegen der sich ständig verbessernden Sicherungsprodukte erforderlich, daß die getroffenen Maßnahmen in regelmäßigen Abständen kontrolliert und an neue Erkenntnisse und Gegebenheiten angepaßt werden.

19.4 „Viren" in EDV-Systemen

In der Vergangenheit konnte man der Presse häufig beunruhigende Meldungen über „Computer-Viren" entnehmen, so z. B., daß ein bestimmter Virus am Freitag, dem 13. Oktober 1989, in Computersystemen aktiv wird. Diese Meldungen haben sich – zumindest für den öffentlichen Bereich – jedoch nicht bestätigt, aber zu einer gewissen Unsicherheit gerade bei PC-Anwendern geführt.

Ein Computer-Virus ist ein Programmteil innerhalb eines Computerprogramms. Dieses Programmteil kopiert sich selbst in weitere Programme hinein.

Das Vorhandensein von Viren setzt voraus, daß Programme geladen werden, die einen Virus enthalten.

Bei den mit Viren infizierten Programmen kann es sich handeln um:

- Standardsoftware, die nach Erstellung einer Kopie verseucht wurde,
- durch eigene Mitarbeiter erstellte Programme,
- Spielprogramme, die ständig kopiert werden und deren Herkunft nicht bekannt ist,
- Billigangebote an Softwareprodukten (Public-Domain-Software), die teilweise unentgeltlich oder gegen einen geringen Kaufpreis gegenüber der Originalsoftware im Programmcode zur Verfügung gestellt werden.

Bekannt ist mittlerweile eine Vielzahl unterschiedlicher Viren, die aus den folgenden Grundfunktionen bestehen:

- einer geheimen Kennung, die es ermöglicht, daß ein Programm nur einmal infiziert wird. Ohne eine solche Kennung würde durch eine mehrfache Infizierung der gleichen Programme frühzeitig die Aufblähung der Programme entdeckt werden, da sie schnell zu groß für den verfügbaren Hauptspeicher würden;
- einem Programmteil, das weitere bisher nicht infizierte Programme sucht und diese durch Einkopieren des Virus infiziert;
- einer Abfrage auf unterschiedliche Bedingungen. Solche Abfragen können das aktuelle Systemdatum sein (z. B. Freitag der 13. und Jahr 1989) oder es werden verborgene Zähler geführt, die bei einer bestimmten Anzahl von Programmdurchläufen den gewollten Schadensablauf herbeiführen.

Bei Erfüllung der abgefragten Bedingungen wird der gewollte Schadensmechanismus in Gang gesetzt. Dieser kann aus einer harmlosen Meldung oder veränderten Funktionen bestehen, die dem Benutzer lediglich lästig sind, er kann aber auch zur Veränderung und Zerstörung von Dateien führen.

Zur Entdeckung von Viren gibt es mittlerweile Virensuchprogramme in unterschiedlicher Funktionsweise.

Wird ein Virus festgestellt, der in seiner Wirkung nicht bekannt ist, kann er nur durch Neuformatieren des Datenträgers sicher entfernt werden. Damit sind alle Daten verloren und alle Programme müssen neu installiert werden. Da nicht bekannt ist, ob auch Datenträger mit Sicherungsbeständen infiziert sind, ist ein Rückgriff auf solche Bestände wenig hilfreich.

Zum Schutz vor Computerviren sollte nur Originalsoftware aus vertrauenswürdiger Quelle eingesetzt und ein kontrollierbarer Softwareimport an den Systemen durchgeführt werden.

Vor allem von Spielprogrammen, die als Kopien von Hand zu Hand weitergegeben werden, geht zur Zeit die größte Gefahr einer Infizierung aus. Daher sind bisher auch Viren in größerem Ausmaß im Homecomputerbereich aufgetreten.

19.5 Ergebnisse örtlicher Feststellungen

19.5.1 Überprüfung eines kommunalen Gebietsrechenzentrums

Die Sicherungsmaßnahmen des Rechenzentrums waren unzureichend. Auf die folgenden schwerwiegenden Mängel wurde hingewiesen:

- Es existierten keine technischen Überwachungsmöglichkeiten außerhalb der Dienstzeit (Bewegungsmelder o. ä.).

- Der Zugang zum Sicherheitsbereich des Rechenzentrums war nur durch einfache Holztüren gesichert.

- Der unbefugte Zugang zum Sicherheitsbereich war durch Mitarbeiter des Vermieters der Gebäude, die im Besitz eines Generalschlüssels sind, auch außerhalb der Dienstzeit ohne Kontrolle möglich.

- Im gesamten Bereich des Maschinensaals, Papierlagers und in der Arbeitsnachbereitung waren keine Brandsicherungen vorhanden.

Das gesamte Datenträgerarchiv mit ca. 2 000 Datenträgern (Magnetbänder und Kassetten) war innerhalb des Maschinensaals untergebracht. Da das Rechenzentrum für eine Vielzahl anderer öffentlicher Stellen die Datenverarbeitung im Auftrag durchführt und somit auch für die Sicherung der Datenbestände verantwortlich ist, wurde darauf hingewiesen, daß ein Störfall angesichts dieser Lagerung von Datenträgern einen erheblichen Schaden verursachen kann.

Die Behebung dieser Sicherheitsmängel wurde von der Stadtverwaltung ständig aufgeschoben mit der Begründung, daß das RZ in ein neues, funktionsgerechtes Gebäude verlegt werde, das über ausreichende Sicherheitseinrichtungen verfüge. Von einem im Grundsatz wenig entwickelten Datenschutzverständnis zeugt aber auch die Tatsache, daß die für den Betrieb des Rechenzentrums erlassene Dienstanweisung – Stand 7. Mai 1975 – über eine Zeitdauer von mehr als zehn Jahren nicht mehr an die veränderte Maschinenausstattung, das veränderte Betriebssystem und die räumlichen Gegebenheiten angepaßt wurde.

19.5.2 Ergebnisse der Überprüfung verschiedener Ämter einer Stadtverwaltung

Automatisiertes Ordnungswidrigkeitsverfahren beim Straßenverkehrsamt:

- Empfehlungen der DSK zur Einführung einer automatisierten Löschung von erledigten Ordnungswidrigkeitsfällen wurden realisiert. Die Löschungen werden vierteljährlich zum Quartalsende durchgeführt.

- Die unzulässige Übermittlung des „Zuzugsdatums" und der „Nationalität" beim Online-Zugriff zum Abruf von Meldedaten der KDZ wurde durch eine entsprechende Programmänderung abgestellt.

- Der Zugriff der Politessen über einen installierten Bildschirm zur automatisierten Fahrzeugzulassungsdatei wurde auf zwei Mitarbeiterinnen der Einsatzleitstelle beschränkt. Der Datenzugriff ist nur mit einem entsprechenden Paßwort möglich.

Stadtkasse und Vollstreckungsstelle

- Die Unterbringung der Stadtkasse und der Vollstreckungsstelle in einem Großraumbüro und die Anordnung der Arbeitsplätze in der Vollstreckungsstelle hatten zur Folge, daß vom Publikum Telefongespräche und persönliche Gespräche über Vollstreckungs- und Pfändungsangelegenheiten mitgehört werden konnten. Den Empfehlungen der DSK wurde entsprochen, indem eine Personalumsetzung vorgenommen und eine Wartezone für die Besucher der Stadtkasse bzw. der Vollstreckungsstelle geschaffen wurde.

- Die Vollstreckungsakten, die zum Zeitpunkt der Überprüfung offen auf den Schränken, die auch als Raumteiler dienten, im Zugangsbereich zur Vollstreckungsstelle abgelegt waren, werden künftig in verschlossenen Schränken aufbewahrt.

- Für einen Online-Zugriff auf Abgabekonten stand für die Sachbearbeiter der Stadtkasse und in der Vollstreckungsstelle nur ein Bildschirm zur Verfügung. Es wurde festgestellt, daß – obwohl jedem Benutzer ein Benutzername und Paßwort zugeordnet war – keine ordnungsgemäßen An- und Abmeldungen vorgenommen wurden. Dies bestätigte auch ein Hinweis auf dem Bildschirm, daß keine Abmeldung zu erfolgen habe. Die zugriffberechtigten Sachbearbeiter wurden angewiesen, künftig nur noch mit eigenem Paßwort auf Abgabekonten zuzugreifen und auch bei kurzfristigen Unterbrechungen den Zugriff abzumelden. Zusätzlich sollen weitere Bildschirme installiert werden um eine bessere Abgrenzung des Benutzerkreises zu erreichen.

- Die Zugriffberechtigung für Sachbearbeiter in der Vollstreckungsstelle wurde auf Anregung der DSK insoweit geändert, als zukünftig nur noch der Zugriff auf Konten möglich ist, gegen deren Inhaber ein Beitreibungsverfahren eröffnet wurde.

19.6 Sicherheit bei der Datenkommunikation

In der Vergangenheit wurde des öfteren darüber berichtet, daß es Hackern gelungen ist, in Datennetze und angeschlossene Rechner einzudringen und dort unbemerkt an Informationen (Datenbestände) zu gelangen.

Der DSK sind für den öffentlichen Bereich rheinland-pfälzischer Verwaltungen keine derartigen Fälle bekannt. Eine gewisse Sicherheit ist dadurch erreicht, daß in den zentralen Rechenzentren Daten vorwiegend unter Verwendung von Standleitungen, auch HfD-Verbindung genannt (HfD = Hauptanschluß für Direktrufverbindung), übertragen werden.

Bei diesen Direktverbindungen können nur die dem Rechenzentrum (Verbindungsrechner) bekannten Endgeräte für eine Datenübertragung eingesetzt werden.

In der Beantwortung einer Kleinen Anfrage Nr. 11/2436 durch das ISM wurde darauf hingewiesen, daß in der Landesverwaltung außer den vorhandenen Standleitungen auch öffentliche Datennetze genutzt werden und ein Eindringen in diese nach dem heutigen Stand der Technik mit vertretbarem Aufwand nicht absolut ausgeschlossen werden kann.

Vor diesem Hintergrund wurde das Ministerium bereits im April dieses Jahres um Mitteilung gebeten, bei welchen automatisierten Verfahren, die dem Landesdatenschutzgesetz unterliegen, welche öffentlichen Datennetze für die Datenübermittlung genutzt werden.

Die Bemühungen der DSK, auch auf anderem Wege nähere Aufschlüsse zu gewinnen, ergaben unterdessen, daß beispielsweise bisher unbekannte Wählverbindungen über öffentliche Datennetze zu ADV-Anlagen öffentlicher Stellen bestehen. Das Ministerium hat trotz Erinnerung bisher noch nicht Stellung genommen.

Bei der Datenübermittlung und bei Online-Zugriffen – insbesondere bei Wählverbindungen – ist eine hohe Verfahrenssicherung dadurch zu erreichen, daß eine Authentisierung (Benutzer, Datenstation) und Autorisierung (Zugriffsrechte) realisiert wird. Eine solche Berechtigungsprüfung ist bisher nicht in allen Online-Verfahren eingeführt, so z. B. für den Zugriff auf das landeseinheitliche EWOIS-Verfahren. Dies hat zur Folge, daß für Abrufe und Veränderungen von Daten nur eine Protokollierung je Endgerät und nicht benutzerbezogen möglich ist. Da in der Praxis häufig mehrere Personen eine Datenstation benutzen, ist nachträglich eine Feststellung des Verantwortlichen nicht mehr möglich, da auch keine schriftlichen Aufzeichnungen über Datenveränderungen und Abrufe vorgenommen werden. Eine maschinelle Protokollierung, wer zu welchem Zeitpunkt welche Veränderung vorgenommen hat, ist schon gem. § 1 Nr. 7 LVO zu § 9 LDatG vorgeschrieben. Entsprechende Protokollierungen der Abrufe sollten nach Auffassung der DSK ebenfalls eingerichtet werden, wenn dies möglich ist. Die Zweckbindung der dann entstehenden Datenbestände für Kontrollzwecke ist jedoch zu gewährleisten.

Für das gleiche Verfahren, in dem einige Kommunalverwaltungen aus Wirtschaftlichkeitsgründen den Online-Zugriff nicht mehr über die bislang genutzten Standleitungsverbindungen, sondern über einen Rechner in der kommunalen Datenzentrale als Vorschaltstelle vornehmen wollten, wurde die DSK um eine Stellungnahme aus datenschutzrechtlicher Sicht gebeten. Nach eingehender Erörterung unter Beteiligung beider Rechenzentren vertrat die DSK die Auffassung, daß für die Übermittlung der EWOIS-Daten über die kommunale Datenzentrale keine grundsätzlichen Bedenken bestehen, wenn die nachfolgenden Voraussetzungen geschaffen sind:

- Es muß durch die kommunale Datenzentrale sichergestellt werden, daß jede weitere angeschlossene Verwaltung nur auf die ihrer regionalen Zuständigkeit unterliegenden Daten zugreifen darf. Weiterhin muß für beide Rechenzentren durch technische Maßnahmen sichergestellt sein, daß den einzelnen abfragenden Behörden nur die Daten (Auskunftsformate oder Änderungsformate) zu Verfügung gestellt werden, die in der Meldedatenübermittlungsverordnung und im landeseinheitlichen Verfahren festgelegt sind.

- Die maschinelle Protokollierung bei der kommunalen Datenzentrale muß nach Abfragen und Änderungen des Datenbestandes gewährleisten, daß der Zeitpunkt, der benutzte Bildschirm und Benutzer aufgezeichnet wird.

- Die Datenübermittlung darf nur über Standleitungsverbindungen erfolgen. Eine Einrichtung von Wählleitungen wurde aus Gründen der Datensicherheit nicht akzeptiert.

19.7 Datenschutzregister, Dienstanweisungen über organisatorische und technische Datensicherungsmaßnahmen

Die Zahl der Anmeldungen zum Datenschutzregister hat sich im Berichtszeitraum um rund 800 auf etwa 3 900 erhöht. Ohne jeden Zweifel ist jedoch die Zahl der tatsächlichen Anwendungen weitaus höher, m. a. W., viele Behörden und andere öffentliche Stellen kommen ihrer Anmeldepflicht nach § 10 LDatG nicht nach. Dies folgt daraus, daß seit Jahren die Zahl der Neuanmeldungen zum Datenschutzregister etwa gleichbleibt, die tatsächlich installierte Rechnerkapazität aber sprunghaft zugenommen hat. Für Anwendungen auf Arbeitsplatzrechnern (Personalcomputern – PC –) liegen weitaus weniger Anmeldungen vor, als nach Kenntnis der DSK aufgrund des tatsächlichen Einsatzes derartige Geräte in der öffentlichen Verwaltung des Landes vorliegen müßten. Oft werden Anmeldungen zum Datenschutzregister verspätet oder unvollständig vorgenommen. Dies kann zur Folge haben, daß die Realisierung der von der DSK geforderten Datensicherungsmaßnahmen erhebliche zusätzliche Kosten verursacht.

Die DSK verkennt nicht, daß Anmeldungen zum Datenschutzregister mit einem gewissen Verwaltungsaufwand verbunden sind, dessen Sinn für die anmeldepflichtigen Stellen oft nicht genügend einsichtig ist. Die Anmeldungen bilden indessen für die Datenschutzarbeit eine wichtige Informationsquelle und sind deshalb im Grundsatz unverzichtbar. Die Bemühungen der DSK, das Anmeldeverfahren so einfach wie möglich zu gestalten, werden verstärkt fortgesetzt. Zur Zeit wird geprüft, ob im Bereich der Anwendung von Arbeitsplatzrechnern Gestaltungsspielraum besteht, den die DSK mit der Einführung eines vereinfachten Anmeldeverfahrens ausfüllen könnte. Im übrigen besteht die unbestreitbare Notwendigkeit, die Novellierung des LDatG auch für eine angemessene Neubestimmung der gesetzlichen Anmeldepflicht zu nutzen.

Eine wichtige Klarstellung wurde durch die Neuordnung des Datenschutzes im Krankenhausbereich (§ 36 LKG) vorgenommen. Die Datenverarbeitung in Krankenhäusern ist – mit Ausnahme der geschäftsmäßigen Datenverarbeitung für fremde Zwecke – nicht anmeldepflichtig. Das Äquivalent dieser grundsätzlichen Freistellung bildet die Dateiübersicht, die von den Datenschutzbeauftragten der Krankenhäuser zu führen ist und die auch der DSK für Prüfungszwecke zur Verfügung steht.

Auch die Dienstanweisungen über technische und organisatorische Datensicherungsmaßnahmen nach § 9 Abs. 2 werden häufig nicht erstellt oder genügen nicht den Anforderungen. Den Empfehlungen der DSK wird bisweilen nur mit großer zeitlicher Verzögerung entsprochen. Eine Landes-Lehr- und Versuchsanstalt beispielsweise wurde im September 1986 gebeten, die vorgelegte Dienstanweisung um Regelungen über die Zugangskontrolle, Eingabekontrolle, Speicherkontrolle, Benutzerkontrolle und Zugriffskontrolle zu ergänzen. Im Februar 1987 erhielt die DSK eine Mitteilung, daß der Vorgang an die zuständige Aufsichtsbehörde, das MLWF, weitergegeben worden sei.

Trotz mehrfacher Erinnerungen hat das Ministerium bis heute keine Dienstanweisung vorgelegt. Es wurde vielmehr wegen „urlaubsbedingter Ausfälle" um Zeitaufschub gebeten.

Zur Problematik von sogen. „Musterdienstanweisungen" vgl. Tz. 10.1.2.5.

20 Sonstige Tätigkeitsbereiche

20.1 Allgemeine Verwaltungsverfahrensfragen (Informantenschutz)

Nicht selten sind Behörden die Adressaten von Beschwerden oder Hinweisen, die andere Behörden oder Personen und Stellen außerhalb des öffentlichen Bereichs betreffen. Die Beschwerden oder Hinweise sind darauf gerichtet, die Behörden zur Wahrnehmung von Aufsichtspflichten anzuhalten, tatsächlichen oder vermeintlichen Mißständen nachzugehen, Genehmigungen zu widerrufen usw.

Für die Behörde als Empfänger solcher Beschwerden oder Hinweise stellt sich die Frage, was weiter zu geschehen hat. Darf sie im Rahmen einzuleitender Recherchen den Namen des Beschwerdeführers oder Hinweisgebers offenbaren, darf sie gar eine Ablichtung des ihr zugegangenen Schreibens weitergeben oder ist ihr dies aus Datenschutzgründen verwehrt?

Eine Beantwortung dieser Fragen durch Anwendung von Vorschriften des Landesdatenschutzgesetzes ist meistens nicht möglich, denn in aller Regel liegen die formalen Anwendungsvoraussetzungen dieses Gesetzes nicht vor. Die Informationsweitergabe erfolgt weder im automatisierten Verfahren noch aus einer Datei.

Ausgangspunkt einer rechtlichen Beurteilung ist vielmehr der im Bereich der öffentlichen Verwaltung geltende Geheimhaltungsgrundsatz, der für das Verwaltungsverfahren in § 30 Verwaltungsverfahrensgesetz gesetzlich geregelt ist. Dabei kann dahingestellt bleiben, ob es sich bei der Aufforderung zur Prüfung von Vorgängen oder bei einer Beschwerde – schon – um ein Verwaltungsverfahren handelt, denn die genannte Vorschrift ist als Ausdruck eines allgemeinen Rechtsgedankens immer dann anzuwenden, wenn keine Sonderregelung besteht (vgl. Kopp, Verwaltungsverfahrensgesetz, RdNr. 2 zu § 30, ähnlich auch Obermayer, RdNr. 46 zu § 29).

Das gesetzgeberische Motiv der genannten Vorschrift liegt darin, dem Bürger die Befürchtung zu nehmen, seine Angaben könnten in falsche Hände gelangen. Die Diskretionsgewißheit der Beteiligten soll ein vertrauensvolles Verhältnis zwischen Verwaltung und Bürger ermöglichen (vgl. Mayer/Borgs, Verwaltungsverfahrensgesetz, RdNr. 2 zu § 30). In Bereichen, in denen die Verwaltung bei der Wahrnehmung ihrer Aufgaben auch auf Informationen aus der Bevölkerung angewiesen ist, sollte alles daran gesetzt werden zu vermeiden, daß die Bereitschaft, den Behörden tatsächliche oder vermeintliche Mißstände vorzutragen, beeinträchtigt wird. Danach ist es im Grundsatz nicht zulässig, die Namen und Anschriften von Informanten weiterzugeben, es sei denn, der Beschwerdeführer oder Hinweisgeber wünscht dies oder er ist mit der Weitergabe einverstanden. In Fällen, die nur unter Preisgabe der Identität des Beschwerdeführers oder Hinweisgebers weiter bearbeitet werden können, sollte dessen Zustimmung eingeholt werden.

In einem konkreten Falle, der an die DSK zur Stellungnahme herangetragen wurde, ging es um die Weitergabe einer Beschwerde, die von einem eingetragenen Verein mit dem Namen „Schutzgemeinschaft gegen Mülldeponie" an das MUG gerichtet wurde. Das Ministerium hatte die Beschwerde an den Deponiebetreiber zur Stellungnahme weitergegeben; dieser stellte gegen die Unterzeichner Strafanzeige wegen übler Nachrede.

Für die datenschutzrechtliche Beurteilung war es in diesem Falle von entscheidender Bedeutung, daß die Beschwerde von einer Organisation vorgebracht wurde, die, wie ihr Name ausweist, Aktivitäten gegen Mülldeponien zum Vereinsziel gemacht hat. Wenn ein Verein in Verfolgung dieses Zieles tätig wird, können entsprechende Aktivitäten und die ihnen zugrunde liegenden Informationsvorgänge nicht als Geheimnis im Sinne des § 30 Verwaltungsverfahrensgesetz angesehen werden. Üblicherweise hat eine Organisation mit entsprechender Zielsetzung kein Interesse daran, daß ihre Aktivitäten geheimgehalten werden. Würde sie im Einzelfall ein solches Interesse erklären, wäre es wohl schutzwürdig; wird es nicht erklärt, kann nach Auffassung der DSK davon ausgegangen werden, daß die Organisation selbst die übermittelten Informationen nicht als Geheimnis ansieht. Dies ergibt sich auch daraus, daß solche Organisationen im allgemeinen – und, wie festgestellt wurde, im konkreten Falle – nicht zögern, ihre Erkenntnisse und die ihnen zugegangenen Informationen der Öffentlichkeit mitzuteilen.

Daß mit der Unterschriftsleistung die nach der Vereinssatzung Handlungsbefugten erkennbar werden, ändert an der rechtlichen Beurteilung nichts. Entsprechende Informationen könnten auch dem Vereinsregister entnommen werden.

Anders war ein Fall zu beurteilen, in dem ein Bürger sich über das Anbringen einer Schranke an einem Waldweg gewehrt hat. Er trug gegenüber dem zuständigen Forstamt vor, diese Schranke sei unter Verletzung geltenden Rechts im Wege der „Kungelei" zwischen dem zuständigen Ortsbürgermeister und dem Jagdausübungsberechtigten eingerichtet worden.

Der über diesen Sachverhalt informierte Forstamtsleiter fertigte einen ausführlichen Telefonvermerk unter Nennung des Informanten und sandte diesen an alle betroffenen Personen und Stellen.

Nach Auffassung der DSK war diese Vorgehensweise nicht gerechtfertigt, da eine sachliche Überprüfung des Vorganges (der Rechtmäßigkeit der Einrichtung einer Schranke) erfolgen kann ohne Aufdeckung der Identität des Bürgers, der sich durch diese Maßnahme gestört fühlte.

20.2 Architektengesetz

Das Architektengesetz ist aufgrund neuer EG-rechtlicher Vorgaben 1988 novelliert worden (verkündet am 4. April 1989, GVBl. S. 71). Die DSK hat im Vorfeld des Gesetzgebungsverfahrens gegenüber dem zuständigen FM darauf hingewirkt, daß die Erhebung und Verarbeitung der Architektendaten durch die Architektenkammer im Gesetz eine möglichst normenklare Grundlage erhält. Sie hat insoweit Empfehlungen formuliert, die im wesentlichen zunächst durch die Landesregierung und dann durch den Landtag akzeptiert worden sind. Bedeutsam ist aus datenschutzrechtlicher Sicht in diesem Zusammenhang insbesondere die Übermittlungsregelung. Soweit Informationen nicht nur Namen, Anschrift und Fachrichtung sowie Tätigkeitsart des Architekten betreffen, dürfen Auskünfte nur an Behörden erteilt werden, und dies nur, wenn die Auskünfte zur Erfüllung der von der Architektenkammer oder der auskunftsersuchenden Behörde wahrzunehmenden Aufgaben erforderlich sind.

Außerdem wurde klargestellt, daß die Auskunftspflichten der Architekten gegenüber ihrer Kammer in einer Satzung der Architektenkammer näher zu bestimmen sind.

20.3 Öffentlichkeitsarbeit

Die von der DSK herausgegebene Schriftenreihe über datenschutzrechtliche Themen „Informationen zum Datenschutz" ist im Berichtszeitraum um ein Heft 4 „Datenschutz im Krankenhaus" erweitert worden. Diese Publikation befaßt sich mit Datenschutzfragen, die für Ärzte und Patienten in den Krankenhäusern in öffentlicher Trägerschaft des Landes Rheinland-Pfalz entstehen. Die Ergänzung des Landeskrankenhausgesetzes um datenschutzrechtliche Vorschriften(§§ 37, 38) hat eine grundsätzlich neue Rechtslage geschaffen, die in der Praxis Fragen hervorgerufen hat, zu deren Klärung das genannte Heft beitragen will.

Heft 1 der Schriftenreihe mit dem Titel „Datenschutzrechtliche Vorschriften" wurde neu aufgelegt: Die große Zahl neuer bereichsspezifischer gesetzlicher Regelungen zum Datenschutz hat eine grundlegende Neubearbeitung erforderlich werden lassen.

Weiterhin wird Heft 2 der Schriftenreihe „Orientierungshilfe zu datenschutzrechtlichen Sicherungsmaßnahmen" überarbeitet. In der neuen 3. Auflage, die in Kürze zur Verfügung stehen wird, werden die Beispiele der Maßnahmen zur besonderen Datensicherung auf PC aufgrund neuer Erkenntnisse und der Möglichkeiten neuer Techniken ergänzt.

Die DSK hat darüber hinaus durch ihre Mitarbeiter an datenschutzrechtlichen Fortbildungsveranstaltungen der verschiedensten Art mitgewirkt. Sowohl im Bereich der Lehrerfortbildung wie im Bereich der informationstechnischen Grundbildung der allgemeinen inneren Verwaltung, aber auch vor Polizeibediensteten, Mitgliedern der Kassenärztlichen Vereinigungen etc. haben Vorträge stattgefunden.

Schließlich hat sich die DSK durch ihre Pressearbeit sowie durch die Verbreitung weiterer Informationsmaterialien (etwa ihrer Tätigkeitsberichte, aber auch anderer Publikationen zum Datenschutz) um die Förderung des Datenschutzbewußtseins bemüht, was Datenschutz im Zeitalter der Informationsgesellschaft bedeutet.

20.4 Zusammenarbeit mit anderen Kontrollinstitutionen

Der Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der DSK Rheinland-Pfalz wechselt jährlich. Im Jahr 1988 hat die DSK, in erster Linie vertreten durch ihr geschäftsführendes Mitglied, diesen Vorsitz wahrgenommen. In drei Sitzungen wurden Themen von genereller Bedeutung erörtert und Beschlüsse gefaßt, die zum Teil in der Anlage abgedruckt sind.

Auch mit dieser Aufgabe war die Geschäftsstelle der DSK stark belastet.

Die Anregung der DSK, daß auch die für den privaten Bereich zuständigen Datenschutzkontrollinstitutionen (die Bezirksregierungen bzw. das ISM als deren Aufsichtsinstanz) einen Tätigkeitsbericht erstatten, auf dessen Grundlage die DSK ihre gem. § 22 LDatG bestehende Koordinierungsfunktion besser wahrnehmen könnte, ist mit wenig überzeugenden Argumenten vom ISM abgelehnt worden (vgl. 11 Tätigkeitsbericht, S. 74; Antwort der Landesregierung auf eine Kleine Anfrage, Drucksache 11/1665).

Mit dem Datenschutzbeauftragten des ZDF hat – wie in den vorangegangenen Berichtszeiträumen – ein Erfahrungsaustausch stattgefunden, dessen Themen in erster Linie dem Tätigkeitsbericht des ZDF-Datenschutzbeauftragten entnommen worden sind. Fragen der Datenerfassung und Verarbeitung bzgl. der Gebührenschuldner sowie des Medienprivilegs standen dabei im Vordergrund.

21 Schlußbemerkung

Dieser Bericht soll, entsprechend dem Gesetzesauftrag, einen Überblick über die wichtigsten Arbeitsergebnisse der DSK vermitteln; er soll aber auch über die Entwicklung der Datenverarbeitung in der öffentlichen Verwaltung des Landes Rheinland-Pfalz sowie über gesetzgeberische Maßnahmen im Bereich des Datenschutzes informieren. Wenn kritische Beiträge überwiegen, so beruht dies auf der in der Vorbemerkung geschilderten Ausgangslage. Es wäre freilich nicht zutreffend, hieraus die Folgerung zu ziehen, daß das Verhältnis zwischen Datenschutzkontrolle und Verwaltung nicht ganz überwiegend von Sachlichkeit und gegenseitigem Verständnis geprägt wäre. Diese Feststellung gilt insbesondere, aber nicht nur, im Verhältnis zum Ministerium des Innern und für Sport.

Zu beklagen ist nach wie vor, daß der Datenschutz gelegentlich als Vorwand für unberechtigte Informationsverweigerungen mißbraucht wird. Beispiele hierfür gibt es nicht nur im kommunalen Bereich, sondern auch bei Landesbehörden aller Ebenen. Die DSK bleibt weiterhin bemüht, dieser Tendenz entgegenzuwirken.

Datenschutz ist ein notwendiges Instrument zur Lösung des Zielkonflikts, einerseits die öffentliche Verwaltung durch Einsatz moderner Kommunikationstechnik möglichst effizient zu machen und andererseits die Persönlichkeitsrechte der Bürger zu wahren. Bisweilen ist es schwierig, dieses Instrument mit der notwendigen Ausgewogenheit einzusetzen. Auch die Datenschutzarbeit ist nicht frei von Fehlern und Irrtümern und sie hat sich der Kritik zu stellen. Nicht gerechtfertigt sind freilich pauschale Angriffe, wie sie gelegentlich ohne sachlichen Grund in der Öffentlichkeit erhoben werden: So müßte beispielsweise erst noch der Nachweis erbracht werden, daß Mißerfolge bei der polizeilichen Fahndung auf einer Überbetonung des Datenschutzes beruhen oder – allgemein ausgedrückt – notwendige und sinnvolle Verwaltungstätigkeit durch den Datenschutz über Gebühr behindert wird.

Abg. Franz-Josef Bischel
(Vorsitzender)

Abg. Dieter Muscheid

Abg. Prof. Heinrich Reisinger

Walter P. Becker,
Direktor beim Landtag Rheinland-Pfalz

Prof. Dr. Walter Rudolf

Anlage 1

Entschließung

der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 26./27. Oktober 1989
über
den Datenschutz in der Europäischen Gemeinschaft

Angesichts der für das Jahr 1993 zu erwartenden Errichtung eines Binnenmarktes in der Europäischen Gemeinschaft zählt der grenzüberschreitende Datenaustausch zu den drängenden, ungelösten Problemen des Datenschutzes.

Eine internationale Datenverarbeitung ist nicht nur eine Grundbedingung für eine gemeinschaftsweite privatwirtschaftliche Tätigkeit. Auch für den öffentlichen Bereich gewinnt die Problematik zunehmend an Bedeutung. Der Abbau der Grenzkontrollen in der Europäischen Gemeinschaft und das vor diesem Hintergrund geschlossene „Schengener Übereinkommen" über die verstärkte informationelle Zusammenarbeit der Polizeibehörden Frankreichs, der Bundesrepublik Deutschland und der Benelux-Staaten sind dafür ein signifikantes Beispiel.

Ebenso werden die technischen Voraussetzungen für internationale Datenübermittlungen immer weiter verbessert. Schon 1993 soll europaweit das digitale, diensteintegrierende Kommunikationsnetz (ISDN) zur Verfügung stehen.

In der Europäischen Gemeinschaft wird die Dynamik der wirtschaftlichen Integration die Entwicklung zu einem „informationellen Großraum" nachhaltig fördern. Dies hat zur Folge, daß die Informationsverarbeitung insbesondere in den Bereichen Umweltschutz, Forschung, Arbeitsmarkt, soziale Sicherung, Statistik und öffentliche Sicherheit erheblich zunehmen wird.

Die Beratungen der Internationalen Konferenz der Datenschutzbeauftragten im August 1989 in Berlin haben erneut gezeigt, daß die auf supranationaler Ebene vorhandenen Regelungen, wie etwa die Europaratskonvention von 1981, zwar wichtige Prinzipien für einen fairen Datenumgang enthalten, aber keineswegs ausreichen, den etwa in der Bundesrepublik Deutschlang oder Frankreich durch das nationale Datenschutzrecht erreichten Stand der Sicherung des informationellen Selbstbestimmungsrechts des Bürgers zu gewährleisten, abgesehen davon, daß eine Reihe von Mitgliedsstaaten der Gemeinschaft die Konvention noch nicht ratifiziert hat.

Besonders bedenklich ist die Untätigkeit der EG im Bereich des Datenschutzes. Rechtsakte der EG verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, etwa im Bereich der Statistik. Die Telekommunikationspolitik der EG ist auf einen forcierten Ausbau europaweit standardisierter und operierender Telekommunikationsdienste und -netze gerichtet. Zwischen den verschiedenen nationalen Datenschutzrechten der Mitgliedsstaaten bestehen im Hinblick auf Verarbeitungsvoraussetzungen, Rechte der betroffenen Personen und Kontrollmöglichkeiten große Unterschiede.

Die Konferenz bekräftigt daher die auf der Internationalen Konferenz in Berlin einmütig erhobenen Forderungen,

- daß bei der Entwicklung und Nutzung grenzüberschreitender Datennetze und Datendienste dem Datenschutz der gleiche Stellenwert zukommen muß, wie der Förderung der technischen Infrastruktur,

- daß die EG ein Gesamtkonzept für die Sicherung des Datenschutzes sowohl in den Mitgliedsländern als auch bei ihren eigenen Aktivitäten entwickeln muß, das insbesondere die Gleichwertigkeit des Schutzniveaus in der gesamten Gemeinschaft herstellt, und

- daß auf der EG-Ebene eine unabhängige Datenschutzinstanz einzurichten ist, die die Institution der Gemeinschaft in allen Datenschutzfragen berät, die Verarbeitung personenbezogener Daten durch die EG-Gremien überwacht, Eingaben von Bürgern entgegennimmt und mit den nationalen Datenschutzorganen zusammenarbeitet.

Die Konferenz der Datenschutzbeauftragten erklärt ihre ausdrückliche Bereitschaft, ihre Kenntnisse und Erfahrungen bei der Realisierung dieser Maßnahmen einzubringen. Ansprechpartner sind dabei zum einen die Organe der Gemeinschaft, insbesondere das Europäische Parlament, zum anderen die an der Willensbildung der EG beteiligten deutschen Behörden des Bundes und der Länder.

Anlage 2

Entschließung

der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 26./27. Oktober 1989
zum
Entwurf eines Schengener Zusatzübereinkommens
über
den schrittweisen Abbau der Grenzkontrollen

1. Am 14. Juni 1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. Dabei knüpften sie den Wegfall der Grenzkontrollen an eine Reihe von Maßnahmen, die die befürchteten Sicherheitsdefizite ausgleichen sollen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Errichtung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung (Schengener Informationssystem – SIS). Dieses System dient vor allem der Ausschreibung zur Festnahme und zur Zurückweisung an der Grenze, der verdeckten Registrierung und der Ermittlung des Aufenthalts von Zeugen im Strafverfahren. Überdies sollen der Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität verstärkt, die ausländer- und asylrechtlichen Entscheidungen vereinheitlicht und ein gemeinsames Verfahren für intensivierte Kontrollen an den Außengrenzen festgelegt werden.

2. Die Vertragsstaaten verpflichten sich in dem Entwurf zum Zusatzübereinkommen, Datenschutzvorschriften für das Schengener Informationssystem entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und der Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten über die Nutzung personenbezogener Daten im Polizeibereich als Mindeststandard zu erlassen. Die Konferenz begrüßt dies und stellt zugleich fest, daß nach dem gegenwärtigen Stand der Verhandlungen auch die in der Erklärung der Datenschutzorgane Frankreichs, Luxemburgs und der Bundesrepublik Deutschland vom 16. März 1989 enthaltenen Forderungen in wesentlichen Bereichen erfüllt werden sollen. Der Vertragsentwurf sieht für das Schengener Informationssystem vor: Auskunfts-, Berichtigungs- und Klagerechte für die Betroffenen; Kontrollorgane auf nationaler und internationaler Ebene; eine Zweckbindung der Daten. Diese Elemente müssen Bestandteile des Zusatzübereinkommens bleiben, bedürfen aber noch der Verbesserung und Ergänzung, damit sich durch den grenzüberschreitenden Datenaustausch keine gravierenden Verschlechterungen für den Datenschutz ergeben.

2.1 Die Datenschutzbeauftragten fordern für das SIS insbesondere die

- Festlegung der Voraussetzungen, nach denen unter Berücksichtigung der Verhältnismäßigkeit (z. B. nach der Schwere der Straftaten) Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden sollen,

- Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten zugreifen dürfen,

- konkrete Beschreibung der Voraussetzungen, unter denen verdeckte Registrierungen erlaubt werden sollen (Straftatenkatalog),

- präzisere Beschreibung der Kriterien, nach denen Zweckdurchbrechungen zur Verhütung einer Straftat mit erheblicher Bedeutung sowie aus schwerwiegenden Gründen der Staatssicherheit erlaubt werden sollen, und

- Aufnahme einer Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren.

2.2 Die Regelungen über den Datenschutz – insbesondere die Rechte der Betroffenen und die Datenschutzkontrolle – müssen auf die im Zusatzübereinkommen vorgesehene konventionelle Verarbeitung personenbezogener Daten ausgedehnt werden. Dies gilt vor allem für den Informationsaustausch in den Bereichen des Ausländerrechts und des Asylverfahrens.

3. Der Entwurf des Zusatzübereinkommens enthält eine pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berücksichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staatssicherheit Hilfe leisten.

   Die Datenschutzbeauftragten weisen vorsorglich darauf hin, daß eine solche Bestimmung nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste darstellt.

4. Der Vertragsentwurf verpflichtet jeden Vertragsstaat, Ausländer aus dritten Staaten an der Grenze zurückzuweisen, wenn ein anderer Vertragsstaat ihn „zur Einreiseverweigerung" ausgeschrieben hat. Es ist nicht vorgesehen, daß der vollziehende Staat die Gründe der Ausschreibung zur Kenntnis nimmt und rechtlich überprüft. Die Datenschutzbeauftragten fordern die verbindliche Festlegung der sachlichen Voraussetzungen solcher Ausschreibungen und die Ermöglichung einer Überprüfung.

5. Die Datenschutzbeauftragten machen darauf aufmerksam, daß das Zusatzübereinkommen den deutschen Gesetzgebern nicht von der dringenden Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens für die polizeiliche Datenverarbeitung verfassungskonforme Rechtsgrundlagen zu schaffen.

6. Bevor die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung nicht erfüllt haben, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, dürfen Daten an diese Staaten auf der Grundlage des Zusatzübereinkommens nicht übermittelt werden.

Anlage 3

Entschließung

**der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
vom 30. Mai 1989
zu den
Entwürfen eines Bundesverfassungsschutzgesetzes (BVerfSchG),
eines MAD-Gesetztes (MADG) und eines BND-Gesetzes (BNDG)**

I.

Mit den von der Bundesregierung vorgelegten Entwürfen sollten die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichspezifischen Rechtsgrundlagen für die Informationsverarbeitung der Verfassungsschutzbehörden und Nachrichtendienste geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, müssen sich neue Gesetze gerade in diesem Bereich in besonderem Maße daran messen lassen, daß in die Freiheitsrechte der Bürger nicht unverhältnismäßig eingegriffen wird. Dieser Vorgabe werden auch die nunmehr vorgelegten Entwürfe in vielerlei Hinsicht nicht gerecht.

II.

1. Da sich der zulässige Umfang der Informationsverarbeitung nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Für den Einzelnen muß erkennbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Die in § 3 Abs. 1 verwendeten Begriffe, wie etwa „Bestrebungen gegen die freiheitliche demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" stellen dies nicht sicher. Insbesondere bleibt unklar,

   - ob der Begriff der Bestrebungen das Handeln einer Mehrzahl von Personen in einem gewissen Grad von Organisiertheit voraussetzt oder auch das Tätigwerden einer einzelnen Person beinhaltet;

   - ob es zulässig sein soll, Informationen auch über solche Bestrebungen zu sammeln und zu speichern, die erkennbar nicht gegen die freiheitliche demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;

   - ob und ggf. in welchem Umfang Informationen über nicht extremistische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung (-sversuche) sind.

   Zur weiteren Umschreibung der Aufgaben könnte auch der Inhalt von § 92 StGB mit herangezogen werden.

2. Bei einer derartig vagen Umschreibung der Aufgaben wäre es um so notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten, je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Spionageabwehr, Extremismus- und Terrorismusbeobachtung, Sicherheitsüberprüfung) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Stattdessen sieht der Entwurf pauschale Befugnisse für den Verfassungsschutz vor. Außerdem fehlen Regelungen darüber ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

3. Unklar ist, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Außerdem muß klargestellt werden, daß die Befugnis zum Einsatz nachrichtendienstlicher Mittel kein genereller Rechtfertigungsgrund für Verstöße gegen Straftatbestände ist, gegen wen sich der Einsatz nachrichtendienstlicher Mittel richten darf und was mit den ggf. dabei über Unverdächtige gewonnenen Daten geschehen darf. Auch im übrigen sollten beim Einsatz nachrichtendienstlicher Mittel, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, entsprechende Schutzrechte wie im Gesetz zu Art. 10 Grundgesetz vorgesehen werden (z. B. Verwertungsverbot, Unterrichtungen).

4. Der Entwurf regelt im wesentlichen lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Informationstechnik es schon heute ermöglicht auch komplexe Datensammlungen – bestehend aus Akten, Dateien und anderen Unterlagen – gezielt mit Hilfe automatischer Verfahren zu erschließen.

5. Bei der Regelung insbesondere für die gemeinsamen Verbunddateien der Verfassungsschutzbehörden sollte auch klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst in Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben. Darüber hinaus ist sicherzustellen, daß in der Datei die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden.

6. Die Frage, ob Einsicht in amtliche Register zulässig sein soll, kann nur bereichsspezifisch geregelt werden. Die Zulässigkeit der Einsichtnahme in Register rechtfertigt nicht die Einrichtung von Online-Anschlüssen.

7. Das Zweckbindungsgebot ist sowohl für Übermittlungen an den Verfassungsschutz als auch für solche durch den Verfassungsschutz nicht ausreichend berücksichtigt. Die nunmehr vorgesehenen Übermittlungseinschränkungen reichen vor allem deshalb nicht aus, weil die übermittelnde Stelle nicht ausdrücklich verpflichtet wird zu prüfen, ob schutzwürdige Belange entgegenstehen. Auch innerhalb des Bundesamtes für Verfassungsschutz darf nicht jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden.

8. Aus dem Trennungsgebot für Polizei- und Nachrichtendienste folgt insbesondere, daß die Übermittlung von Daten, die die Polizei unter Einsatz dem Verfassungsschutz vorenthaltener Befugnisse, z. B. bei Hausdurchsuchungen, gewonnen hat, nur nach Maßgabe einschränkender Verwertungsregelungen erfolgen darf. Die Ansatzpunkte, die im Entwurf der letzten Legislaturperiode enthalten waren, sollten wieder aufgegriffen werden.

   Die Informationshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

9. Es fehlen auch befriedigende Löschungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, sollten schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festgelegt werden. Dabei sollte zwischen den einzelnen Aufgabenbereichen des Bundesamtes für Verfassungsschutz unterschieden werden.

10. Die Einschränkungen des Auskunftsrechts der Bürger sind bereichsspezifisch im Bundesverfassungsschutzgesetz zu regeln. Ein Auskunftsanspruch besteht in der Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht. Im übrigen bedarf es einer Abwägung im Einzelfall. Die Ablehnung ist gegenüber dem Betroffenen soweit zu begründen, daß er sachgerecht darüber entscheiden kann, ob und welche Rechtsmittel er einlegen will. Außerdem ist der Betroffene auf sein Recht hinzuweisen, sich an den Datenschutzbeauftragten zu wenden.

11. Die Datenschutzbeauftragten begrüßen es, daß die Beteiligung des Verfassungsschutzes an Sicherheitsüberprüfungen und Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes in einem eigenen Geheimschutzgesetz geregelt werden sollen. Sofern über die Sicherheitsüberprüfung hinaus eine Mitwirkung an anderen Verfahren für unabdingbar gehalten wird, sind diese gesetzlich zu regeln.

12. Soweit die Entwürfe für ein MAD-Gesetz und ein BND-Gesetz auf das Bundesverfassungsschutzgesetz verweisen, gilt die hierzu geäußerte Kritik. Die in den Entwürfen vorgesehene Verweisungstechnik erhöht für den Bürger die Schwierigkeit, aus den Gesetzen klar zu erkennen, welche personenbezogenen Daten die Dienste bei welcher Gelegenheit über ihn verarbeiten dürfen. Darüber hinaus bestehen Zweifel, ob die für das Bundesamt für Verfassungsschutz vorgesehenen Befugnisse pauschal auch für den Militärischen Abschirmdienst notwendig sind, der als Teil der Streitkräfte ein gegenüber dem Bundesamt für Verfassungsschutz deutlich unterschiedliches Operationsgebiet hat.

Anlage 4

Entschließung

der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
vom 4. April 1989 in Saarbrücken
zum Entwurf eines Gesetzes
zur Änderung und Ergänzung des Strafverfahrensrechts
(Strafverfahrensänderungsgesetz vom 3. November 1988)

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im übrigen unvollständig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren Beschluß vom November 1986 folgende Kritikpunkte hervor:

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

   – Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeitsrecht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z. B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über „Kontakt- und Begleitpersonen", „andere Personen" und „Dritte" werden dem nicht gerecht.

   – Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z. B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte „besondere Fahndungs- und Ermittlungsmethoden" dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.

   – Der Entwurf betont zu recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen; die bloße Anknüpfung an den Begriff der „Straftat mit erheblicher Bedeutung" ohne weitere Differenzierung reicht nicht aus.

   – Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Zwecke verwendet werden sollen.

   – Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt – von besonderen Eilfällen abgesehen – nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt; erhobene Daten sind zu löschen.

   – Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben erforderlich sind.

2. Zu den besonderen Regelungen über die Datenverarbeitung

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

- Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für „Zwecke des Strafverfahrens", für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.

- Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltschaftlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wen die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.

- Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.

- Die vorgesehene Speicherung von Daten über Personen, die „bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen", oder die „Opfer eine Straftat werden könnten", gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z. B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.

- Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. Zur Akteneinsicht

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. Fehlende Regelungen

Regelungsbedürftig sind außerdem vor allem:

- die engere Festlegung der Zulässigkeit erkennungsdienstlicher Behandlungen und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnen Daten,

- die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen im Strafverfahren,

- der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

Anlage 5

Entschließung

**der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 26./27. Oktober 1989
über
Genomanalyse und informationelle Selbstbestimmung**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquête-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Gentechnologie bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der möglichen Folge gesellschaftlicher Ausgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundsätze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.

2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrekken. Im Falle eines Widerrufs sind die gewonnen Informationen zu löschen oder an den Betroffenen herauszugeben.

3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.

4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.

5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genonmanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.

6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.

8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muß vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

Anlage 6

Zur Neuordnung des Personalaktenrechts

Stellungnahme der DSK Rheinland-Pfalz zum Referentenentwurf eines Gesetzes zur Neuordnung des Personalaktenrechts im Bundesbeamtengesetz und Beamtenrechtsrahmengesetz vom 16. August 1989

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat bereits in einer Entschließung vom 28. März 1984 zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts betont, daß das Recht der Erhebung und Verarbeitung von Arbeitnehmerdaten dringend der gesetzlichen Neuregelung bedarf: Wenn der Arbeitnehmer wegen seiner Abhängigkeit von Arbeitsplatz und Einkommen, zur Sicherung seiner Existenz, also praktisch unter Zwang, personenbezogene Daten im Rahmen des Beschäftigungsverhältnisses angibt oder deren Erhebung und Verarbeitung durch den Arbeitgeber duldet, so muß der damit verbundenen Gefährdung seiner Persönlichkeitsrechte durch eine präzise gesetzliche Bestimmung der Verwendungszwecke der erhobenen Daten, des Schutzes vor Zweckentfremdung durch Weitergabe- und Verwertungsverbote, vor allem aber der Beschränkung auf das erforderliche Datenminimum entgegengewirkt werden.

Dies gilt grundsätzlich auch für den öffentlichen Dienst.

Die Datenschutzkommission begrüßt daher die Absicht der Bundesregierung, noch in dieser Legislaturperiode des Deutschen Bundestages auf der Grundlage des Berichts der interministeriellen Arbeitsgruppe zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst durch eine Änderung und Ergänzung des Bundesbeamtengesetzes, die Leitbildfunktion für weitere anstehende Gesetzesänderungen hat, das Personalaktenrecht auf neue gesetzliche Grundlagen zu stellen.

Zwar handelt es sich hierbei um einen Teilaspekt der Problematik. Die Feststellung der interministeriellen Arbeitsgruppe, die Entwicklung habe einen Punkt erreicht, an welchem der Umgang mit dem Recht für alle Beteiligten zu immer größeren Schwierigkeiten führe und an dem rechtsstaatlich vorrangige Ziele wie Rechtsklarheit und Rechtssicherheit auf Dauer verloren zu gehen drohten, gilt nicht nur für das Personalaktenrecht. Sie gilt – zumindestens aus datenschutzrechtlicher Sicht – für das gesamte Recht des öffentlichen Dienstes, darüber hinaus auch für den Arbeitnehmerdatenschutz schlechthin.

Gleichwohl erkennt die Datenschutzkommission an, daß eine datenschutzrechtliche Novellierung des Personalaktenrechts ein erster wichtiger Schritt in die gebotene Richtung wäre.

II.

Die Zielsetzung des Bundesministeriums des Innern, mit dem Gesetz zur Neuordnung des Personalaktenrechts nicht „punktuelle Korrekturen", sondern auf der Grundlage einer „umfassenden Gesamtschau . . . zukunftsorientierte Regelungen zu schaffen", kann aus datenschutzrechtlicher Sicht nur gutgeheißen werden. Die „zukunftsorientierten Regelungen" dürfen sich allerdings nicht darin erschöpfen, die Verarbeitung personenbezogener Beamtendaten mittels „neuer Technologien" nunmehr spezialgesetzlich zu sanktionieren. Auch die „Gesamtschau" bleibt lückenhaft, wenn die erheblichen Konsequenzen kaum erkannt, geschweige denn gezogen werden, die sich aus der Rechtsprechung zum Recht auf informationelle Selbstbestimmung auch gerade für die gesetzliche Neuordnung des Personalaktenrechts ergeben. Anknüpfungspunkt jeder Novellierung sollte nicht der „materielle, mit dem Einsichtsrecht korrespondierende Personalaktenbegriff so, wie er sich als Ergebnis umfangreicher Judikatur und rechtswissenschaftlicher Diskussion darstellt", sein (Bericht der interministeriellen Arbeitsgruppe S. 2), sondern die Achtung und der Schutz des Grundrechts auf informationelle Selbstbestimmung.

Dies schließt die „Verhinderung einer mißbräuchlichen und unangemessenen Verwendung von Daten" (Bericht S. 6) durchaus ein, geht aber erheblich darüber hinaus.

Da dieser Punkt von ausschlaggebender Bedeutung für die Beurteilung des Gesetzentwurfs ist und Auswirkungen auf zahlreiche Einzelfragen hat, soll näher auf ihn eingegangen werden:

1. Das „Grundrecht auf informationelle Selbstbestimmung" gewährleistet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Hieraus folgt, daß die Erhebung, Speicherung und sonstige Verarbeitung personenbezogener Daten durch den Staat – unabhängig davon, ob in Dateien oder Akten (BVerfG 1 BvL 49/86) – nur dann zulässig ist, wenn sie aufgrund einer verfassungsgemäß zustandegekommenen gesetzlichen Befugnisnorm erfolgt, aus der sich die Voraussetzungen und der Umfang der Beschränkungen des Grundrechts klar und für den Betroffenen erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (BVerfG 2 BvR 522/87). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Dieser

mit Verfassungsrang ausgestattete Grundsatz folgt bereits aus dem Wesen der Grundrechte selbst, die als Ausdruck des allgemeinen Freiheitsanspruchs des Bürgers gegenüber dem Staat von der öffentlichen Gewalt jeweils nur soweit beschränkt werden dürfen, als es zum Schutz öffentlicher Interessen unerläßlich ist.

2. Vorstehendes gilt auch im „besonderen Gewaltverhältnis" (Sonderstatusverhältnis), das keine eigene implizite Grundrechtsschranke darstellt (BVerfG 2 BvR 41/71). Der Beamte „steht zwar in einem freiwillig übernommenen Dienst- und Treueverhältnis zu seinem Dienstherrn und ist deshalb mit besonderen, über die allgemeinen Bürgerpflichten hinausgehenden Pflichten dem Staat gegenüber belastet. Zugleich ist er jedoch Bürger, der seine Grundrechte gegenüber dem Staat, mithin auch gegenüber seinem Dienstherrn, geltend machen kann. Dieser Konflikt zwischen der Garantie der individuellen Freiheit und der Garantie eines für die Erhaltung dieser Freiheit unentbehrlichen Staatsapparates muß bei der Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung, wie bei anderen Grundrechten auch, in der Weise gelöst werden, daß nur solche Grundrechtsbeschränkungen zulässig sind, die durch Sinn und Zweck des konkreten Dienst- und Treueverhältnisses des Beamten gefordert werden" (OVG Münster 1 A 2877/84).

3. Weder der Schutz öffentlicher Interessen noch der Sinn und Zweck des beamtenrechtlichen Dienst- und Treueverhältnisses, ja nicht einmal „die Erhaltung der Funktionsfähigkeit des Personalaktenwesens" (Ziffer 2 der Begründung zum Gesetzentwurf) erfordert es, daß über jeden Beamten eine als „Personalakte" bezeichnete (manuelle oder automatisierte) Sammlung auch solcher Daten angelegt wird, die „die persönlichen Verhältnisse des Beamten zum maßgeblichen Bezugspunkt haben" (Ziffer 4 der Begründung zum Gesetzentwurf), also z. B. Ehescheidungsurteile, um – entsprechend einem vom Bundesverwaltungsgericht in ständiger Rechtsprechung betonten Grundsatz – „ein möglichst vollständiges Bild von der Persönlichkeit des Beamten zu ergeben" (BVerwG 6 C 30.72).

   Die Registrierung und Katalogisierung der Persönlichkeit sind mit der Würde des Menschen unvereinbar (BVerfG 1 BvR 209/83). Einen hergebrachten Grundsatz des Berufsbeamtentums des Inhalts, daß für Beamte etwas anderes gilt, gibt es nicht. Eine gesetzliche Regelung, die die umfassende, vollständige Verdatung der persönlichen Verhältnisse und der Persönlichkeit jedes einzelnen Beamten mittels seiner Personalakte verlangt oder gestattet oder auch nur nicht verhindert, wäre weder erforderlich noch verhältnismäßig noch mit dem unmittelbar aus der Verfassung wirkenden (BVerfG 1 BvR 962/87) Anspruch des Beamten auf Achtung seines informationellen Persönlichkeitsrechts vereinbar, und daher verfassungswidrig.

4. Auch von den „persönlichen Verhältnissen" und der „Persönlichkeit" des Beamten abgesehen, ist der Grundsatz der Lückenlosigkeit und Vollständigkeit der Personalakte jedenfalls in der Ausprägung, die er aufgrund der Rechtsprechung des Bundesverwaltungsgerichts in der Praxis gefunden hat, mit dem Grundrecht auf informationelle Selbstbestimmung schwerlich vereinbar. Zum Selbstzweck erhoben, führt er zu einer Dokumentation sämtlicher Vorgänge eines Beamtenlebens, die einem Archivar im Sinne der „historischen Richtigkeit" (BVerwG 6 C 43.76) wohl anstehen mag, zum „Schutz öffentlicher Interessen" oder „nach Sinn und Zweck des beamtenrechtlichen Dienst- und Treueverhältnisses" aber weder geboten noch erforderlich ist und im übrigen den von den Rechnungshöfen des Bundes und der Länder mit Recht geforderten Bemühungen um eine Verringerung des Personalaktenbestandes entgegenwirkt.

   Beispielhaft hierfür mag die Entscheidung einer Dienststelle stehen, die nach dem Freispruch eines Beamten in zweiter und dritter Instanz die Anklageschrift sowie die drei ergangenen Urteile mit der Begründung zur Personalakte nahm, dies sei durch den Grundsatz der Vollständigkeit der Personalakte geboten und nur so könne dokumentiert werden, aus welchem Grund gegen den Beamten nicht disziplinarrechtlich vorgegangen worden sei. Auf diese Art und Weise wird auf Kosten des Persönlichkeitsrechts des Betroffenen ein zwar „lückenloses", aber widersprüchliches, im Ergebnis zwiespältiges oder sogar falsches Bild festgehalten. So auch, wenn eine verwaltungsgerichtliche Entscheidung eine streitige Beurteilung für gegenstandslos erklärt und daraufhin eine neue Beurteilung erstellt wird, nach dem Grundsatz der „Vollständigkeit der Personalakte" jedoch der gesamte Vorgang einschließlich der ersten, unzutreffenden Beurteilung zur Personalakte genommen wird. Zur rechtmäßigen Aufgabenerfüllung der Dienststelle ist dies gewiß nicht erforderlich.

5. Die Achtung vor dem Grundrecht auf informationelle Selbstbestimmung (und vor der Rechtsprechung des Bundesverfassungsgerichts) verlangt, daß sich die gesetzliche Neuregelung des Personalaktenrechts unter deutlicher Abwendung von solchen überholten, aus verfassungsrechtlicher und datenschutzrechtlicher Sicht nicht länger hinnehmbaren Grundsätzen ausschließlich daran orientiert, welche Informationen in einem konkreten Zusammenhang mit dem konkreten Beamtenverhältnis stehen, d. h. die Rechtsstellung, die dienstliche Eignung, Verwendung oder Tätigkeit des Beamten betreffen sowie zur Begründung, Durchführung und Abwicklung des Dienstverhältnisses, insoweit also zur rechtmäßigen Aufgabenerfüllung des Dienstherrn erforderlich sind und folglich zur Personalakte genommen werden müssen und dürfen.

III.

Die Datenschutzkommission verkennt nicht, daß der Gesetzentwurf den vorstehenden Erwägungen näher steht, als manche Anregung der interministeriellen Arbeitsgruppe. So wird begrüßt, daß die Forderungen der Arbeitsgruppe zur „Vollständigkeit" der Personalakte („die Personalakte soll vollständig und lückenlos Aufschluß über den beruflichen Werdegang und insoweit über die Person des Beamten geben") in den Gesetzentwurf keinen Eingang gefunden haben. Ebenso weist die Beschränkung der aufzunehmenden Vorgänge über persönliche Verhältnisse des Beamten auf solche, die „mit dessen Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen", in die richtige Richtung. Um eine wirklich zukunftsorientierte, endlich Klarheit schaffende Regelung zu erreichen, sollten solche positiven Ansätze jedoch konsequent zu Ende gedacht werden.

Im einzelnen:

1. Bei der Beschreibung des Personalakteninhalts (§ 90 Abs. 1 BBG) sollte jeder Hinweis auf die „persönlichen Verhältnisse des Beamten" unterbleiben. Soweit auf solche in der Rechtsprechung, etwa des Bundesverfassungsgerichts zur Einstellungsüberprüfung oder zur Sicherheitsüberprüfung (BVerfG 2 BvL 13/73 und BVerfG 2 BvR 522/87), Bezug genommen wird, geht es fast stets zugleich um dienstliche Belange, so in den genannten Fällen um die Verfassungstreue des Beamten als Ausdruck seiner Treuepflicht und damit Teil seiner dienstlichen Eignung. Der Verzicht auf die Erwähnung der „persönlichen Verhältnisse" schließt also deren Berücksichtigung unter dienstlichen Gesichtspunkten (im Rahmen des Erforderlichkeitsgrundsatzes) nicht aus, setzt jedoch ein Signal.

   Die Bestimmung könnte danach wie folgt formuliert werden:

   „Über jeden Beamten ist eine Personalakte zu führen. Zur Personalakte gehören alle Vorgänge, die die Rechtsstellung, die dienstliche Eignung, Verwendung oder Tätigkeit des Beamten betreffen, soweit dies zur Begründung, Durchführung und Abwicklung des Dienstverhältnisses erforderlich ist."

2. Der Ansatz des Gesetzentwurfs, die Sammlung einiger bestimmter, besonders sensitiver Unterlagen nicht als Bestandteil der Personalakte anzusehen, obwohl sie „die persönlichen oder dienstlichen Verhältnisse des Beamten berühren (§ 90 Abs. 1 BBG), wird begrüßt. Dem Entwurf zufolge soll er nicht für Beihilfeakten gelten. Der Inhalt der Beihilfeakte ist jedoch nicht weniger sensitiv als der der vom Sozialgeheimnis geschützten Kindergeldakte. Auch Beihilfen sind im weiteren Sinne „Sozialleistungen" des Dienstherrn. Die Funktion der Beihilfestelle ist derjenigen einer Betreibskrankenkasse zu vergleichen. Der Schutz der zu einem bestimmten Zweck preisgegebenen Beihilfedaten gegen Zweckentfremdung kann daher nicht hoch genug angesetzt werden. Dies würde es nahelegen, Beihilfevorgänge ebenso wie Kindergeldvorgänge nicht zur Personalakte zu nehmen und entsprechende Schutzvorschriften zu schaffen. Solange solche fehlen, sind Beihilfeakten aber zumindest nicht „grundsätzlich", sondern stets getrennt zu führen und zu bearbeiten.

3. Die Datenschutzkommission begrüßt die Absicht des Gesetzentwurfs, den innerbehördlichen Zugriff auf die Personalakte gesetzlich einzuschränken (§ 90 Abs. 5 BBG), hält jedoch eine Ergänzung der Bestimmung für erforderlich. So gehören Vorgesetzte nicht zu den „im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten". Daß sie Zugang zur Personalakte haben, ist keineswegs selbstverständlich, vielmehr bei Fachvorgesetzten zur rechtmäßigen Aufgabenerfüllung nicht erforderlich und daher unzulässig. Auch kann nicht jeder „Bearbeitungszweck" den Zugang zur Personalakte rechtfertigen.

   Die Datenschutzkommission schlägt daher folgende Formulierung vor:

   „Zugang zur Personalakte haben nur Dienstvorgesetzte und die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten, soweit dies zu personalrechtlichen Bearbeitungszwecken oder zu Zwecken der Personalplanung erforderlich ist."

4. Der Vorschlag des Gesetzentwurfs, dem Beamten ein Recht zur Äußerung vor der Aufnahme von Beschwerden und Behauptungen in die Personalakte zu geben, bei deren Lektüre ein objektiver Leser von außerhalb der Dienststelle negative Folgerungen für den Beamten ziehen könnte, die mithin für ihn ungünstig sind oder ihm nachteilig werden können (§ 90 Abs. 2 BBG), wird begrüßt. Er entspricht nicht nur den Grundsätzen der informationellen Selbstbestimmung, sondern auch dem Grundsatz der Personalaktenwahrheit. Die Formulierung des Gesetzentwurfs ist jedoch unvollständig. Nicht nur Beschwerden und Behauptungen können solche Wirkungen auslösen.

   Die Datenschutzkommission schlägt daher folgende Formulierung vor:

   „Vor der Aufnahme von Beschwerden, Behauptungen, Beurteilungen und sonstigen Unterlagen, die für den Beamten ungünstig sind oder ihm nachteilig werden können, ist er zu hören; seine Äußerung ist zur Personalakte zu nehmen."

5. Die Datenschutzkommission begrüßt es, daß der Gesetzentwurf die Führung von Nebenakten regelt (§ 90 Abs. 4 BBG), die praktisch unumgänglich, in der Vergangenheit jedoch immer wieder Gegenstand von Auseinandersetzungen gewesen ist. Nach dem Erforderlichkeitsprinzip sollte der Inhalt dieser Nebenakten aber von vornherein gesetzlich eingegrenzt werden.

   Die Datenschutzkommission empfiehlt folgende Formulierung:

   „Nebenakten (Vorgänge aus der Grundakte oder den Teilakten) können geführt werden, wenn die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist oder mehrere personalverwaltende Behörden für den Beamten zuständig sind; Nebenakten dürfen nur solche Vorgänge enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der anderen Behörde zwingend erforderlich ist; ein Verzeichnis der Nebenakten ist zur Grundakte zu nehmen."

6. Die Absicht des Gesetzentwurfs, das Recht auf Einsicht in die Personalakte gesetzlich zu konkretisieren (§ 90 a BBG), wird begrüßt. Kleinliche Einschränkungen („soweit dienstliche Gründe nicht entgegenstehen") sind dem Recht auf informationelle Selbstbestimmung unangemessen und sollten daher, zumindest im Gesetz, unterbleiben. Sonderregelungen für „andere als die in Satz 1 und 2 genannten Personen" (§ 90 a Abs. 2 und 3 BBG) erscheinen rechtssystematisch unangebracht oder – angesichts des verfassungsrechtlich ohnehin abgesicherten Zweckbindungsgrundsatzes – entbehrlich.

   Behörden sollten generell nicht „die Personalakte" (d. h. einschließlich sämtlicher Teilakten, wie Beihilfeakte, Urlaubsakte, Reisekostenakte usw.) vorgelegt werden dürfen (§ 90 a Abs. 4 BBG), sondern nur deren zur (konkreten) rechtmäßigen Aufgabenerfüllung jeweils erforderliche Teil, sofern nicht eine Auskunft genügt (vgl. S. 25 der Begründung zum Gesetzentwurf). Nicht genügend normenklar ist es, bei der Vorlage bzw. Auskunftserteilung eine Abwägung des „berechtigten Interesses" der ersuchenden Behörde mit den „schutzwürdigen Interessen des Beamten oder berechtigten Belangen des Dienstherrn" vorzusehen. Auch Auskünfte an Dritte aus der Personalakte eines Beamten (§ 90 a Abs. 5 BBG) haben besondere Eingriffsqualität und sollten deshalb präziser definiert werden.

   Die Datenschutzkommission schlägt vor, § 90 a BBG wie folgt zu formulieren:

   „(1) Der Beamte hat, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständige Personalakte.

   (2) Einem Bevollmächtigten des Beamten ist Einsicht in die Personalakte zu gewähren. Dies gilt entsprechend für die Hinterbliebenen des Beamten, wenn sie ein berechtigtes Interesse darlegen, und für deren Bevollmächtigte.

   (3) Einsicht in die Personalakte wird durch die personalaktenführende Stelle bei ihr oder der von ihr bestimmten Behörde gewährt. Es können Auszüge, Abschriften oder Ablichtungen gefertigt werden.

   (4) Behörden darf nur im jeweils erforderlichen Umfang die Personalakte vorgelegt oder Auskunft aus ihr erteilt werden. Reicht die Einsichtnahme in die Hauptakte oder eine Teilakte aus, so ist die Vorlage hierauf zu beschränken. Auskunftserteilung hat Vorrang gegenüber der Vorlage. Die Vorlage oder die Auskunftserteilung an eine personalverwaltende Behörde desselben Geschäftsbereichs ist ohne Einwilligung des Beamten zulässig, sofern es sich um eine im Rahmen der Dienstaufsicht weisungsbefugte Behörde handelt oder soweit dies zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist. Die Vorlage oder die Auskunftserteilung an eine personalverwaltende Behörde eines anderen Geschäftsbereichs desselben Dienstherrn oder eines anderen Dienstherrn bedarf der Einwilligung des Beamten.

   (5) An Dritte dürfen Auskünfte nur mit Einwilligung des Beamten oder aufgrund einer besonderen gesetzlichen Befugnisnorm erteilt werden."

7. Nicht nur Beschwerden, die sich als unbegründet, und Tatsachenbehauptungen, die sich als falsch erwiesen haben, sind mit Zustimmung des Beamten aus der Personalakte zu entfernen und zu vernichten (§ 90 b Abs. 1 BBG), sondern – nach dem Erforderlichkeitsgrundsatz der informationellen Selbstbestimmung wie dem Grundsatz der Personalaktenwahrheit – sämtliche Unterlagen, die entweder gar nicht zur Personalakte hätten genommen werden dürfen oder aber sich nachträglich als zur rechtmäßigen Aufgabenerfüllung nicht erforderlich erweisen. Beispiele wurden bereits genannt. Hierzu mögen auch die unter § 90 b Abs. 2 bzw. Abs. 3 BBG vorgesehenen Regelungen gerechnet werden, deren Tendenz begrüßt wird.

   Die Datenschutzkommission schlägt folgende Formulierung des Abs. 1 vor: „Beschwerden, Behauptungen, Beurteilungen und sonstige Unterlagen, die sich nachträglich als unrichtig erwiesen haben oder deren Kenntnis zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich ist, sind mit Zustimmung des Beamten aus der Personalakte zu entfernen und zu vernichten."

8. Der ärztlichen Schweigepflicht unterliegende Vorgänge, die beim Personalärztlichen Dienst/Sozialen Dienst/Polizeiarzt geführt werden, sollten ausnahmslos der Einsichtnahme durch den Behördenleiter, dessen Vertreter sowie die mit der Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten entzogen bleiben.

   Die Datenschutzkommission empfiehlt eine entsprechende Ergänzung des Gesetzentwurfs.

9. Müssen Vorgänge, die auch andere Bedienstete betreffen, zur Personalakte genommen werden, so sind deren personenbezogene Daten unleserlich zu machen.

   Die Datenschutzkommission empfiehlt eine entsprechende Ergänzung des Gesetzentwurfs.

10. Die im Gesetzentwurf vorgesehene Begrenzung der Aufbewahrung von Vorgängen über Beihilfen, Unterstützungen, Urlaub, Erkrankungen, Trennungsgeld, Umzugskosten und Reisekosten auf maximal fünf Jahre (§ 90 c Abs. 2 BBG) wird von der Datenschutzkommission begrüßt, da eine längere Aufbewahrung nicht zur rechtmäßigen Aufgabenerfüllung erforderlich erscheint und dann unzulässig wäre.

IV.

Die Datenschutzkommission begrüßt es, daß der Gesetzentwurf die Vorschläge der interministeriellen Arbeitsgruppe zur mikroverfilmten Führung von Personalakten (S. 73 ff. des Berichts) nicht aufgegriffen hat. Die aus wirtschaftlichen Gründen wünschenswerte Reduzierung des Personalaktenbestandes sollte durch Beschränkung des Personalakteninhalts auf das in den Grenzen der Verhältnismäßigkeit und informationellen Selbstbestimmung zur rechtmäßigen Aufgabenerfüllung Erforderliche angestrebt, nicht aber durch mikrotechnische Hilfsmittel letztlich unterlaufen werden.

V.

Die Datenschutzkommission hält die im Gesetzentwurf vorgesehene Regelung (§ 90 d BBG) der automatisierten Verarbeitung personenbezogener Daten von Beamten für unzureichend. Sie teilt zwar die Auffassung, daß eine bereichsspezifische gesetzliche Regelung unumgänglich und – nicht nur im Bundesbeamtengesetz – überfällig ist. Noch immer leiten Bund und Länder, soweit sie ihre Datenschutzgesetze oder beamtenrechtlichen Bestimmungen nicht novelliert oder, teils durch Ausführungsbestimmungen, präzisiert haben, die Befugnis zur automatisierten Verarbeitung personenbezogener Daten der Mitarbeiter des öffentlichen Dienstes aus Vorschriften wie §§ 22 ff. BDSG ab, die weder präzise noch normenklar sind und schon deshalb den verfassungsrechtlichen Anforderungen an Befugnisnormen für Eingriffe in die informationelle Selbstbestimmung nicht entsprechen. Zutreffend betont daher sowohl der Bericht der interministeriellen Arbeitsgruppe wie die Begründung des Gesetzentwurfs die Notwendigkeit einer verfassungskonformen Neuregelung.

Die vorgeschlagene Fassung des § 90 d BBG wird jedoch weder dieser Zielsetzung noch dem Bekenntnis der Bundesregierung (S. 10 der Begründung des Gesetzentwurfs) gerecht, „keine Personalinformationssysteme einzuführen, die sich als umfassendes Kontrollinstrument oder dazu eignen, Persönlichkeitsprofile zu erstellen." Bedenklich sind sowohl die vorgesehenen Regelungen über die automatisierte Verarbeitung und Nutzung medizinischer und psychologischer Daten oder die „personenbezogene Verhaltens- oder Leistungskontrolle", die hiermit erstmals bereichsspezifisch sanktioniert würde, als auch der (anhängende) Hinweis auf automatisierte Abrufverfahren, der eine präzise Regelung von Online-Zugriffen im Gesetz selbst nicht ersetzen kann. Die Begründung des generellen Verzichts auf Vorschriften über die Erhebung, Verarbeitung und Nutzung sowie den technisch-organisatorischen Schutz automatisiert geführter Beamtendaten (dies sei im Bundesdatenschutzgesetz geregelt, S. 11 und 14 der Begründung) überzeugt schon deshalb nicht, weil damit auf Vorschriften abgestellt wird, deren künftige Fassung derzeit noch niemand kennt. Ein „Höchstmaß an Sicherheit" (S. 11 der Begründung) wird hierdurch nicht erreicht, den eingehenden Vorschlägen der interministeriellen Arbeitsgruppe (S. 101 ff. des Berichts) kaum Rechnung getragen.

Angesichts solcher Mängel hält die Datenschutzkommission eine grundlegende Überarbeitung der gesamten Bestimmung für unumgänglich.

Anlage 7

Anforderungen an die Abschottung kommunaler Statistikstellen

1. Nach § 5 Abs. 2 i. V. m. § 4 Abs. 2 und § 8 Abs. 4 Landesstatistikgesetz sind die für die Durchführung von Bundes-, Landes- und Kommunalstatistiken zuständigen Stellen der Gemeinden räumlich, organisatorisch und personell von anderen, mit Aufgaben des Verwaltungsvollzugs befaßten Stellen, zu trennen, solange Einzelangaben vorhanden sind. Die Trennung (Abschottung) ist ferner gefordert als Voraussetzung für die Übermittlung von Einzelangaben nach § 14 Abs. 1 Volkszählungsgesetz sowie für die Übermittlung von Einzelangaben aus anderen Bundesstatistiken nach § 16 Abs. 5 Bundesstatistikgesetz an die Gemeinden.

2. Die nach den Bestimmungen des § 4 Abs. 2 Landesstatistikgesetz von anderen Verwaltungsstellen abgeschottete Stelle muß nicht ständig, sondern nur solange eingerichtet sein, wie erhobene oder übermittelte Einzelangaben vorhanden sind. Sofern Daten auf einem Niveau aggregiert sind, das ein Identifizierungsrisiko ausschließt, oder Einzelangaben so anonymisiert sind, daß sie den Befragten oder Betroffenen nicht mehr zugeordnet werden können, ist eine Verarbeitung außerhalb der abgeschotteten Stelle zugelassen.

3. Die Abschottungsmaßnahmen müssen verhältnismäßig sein. Die Sensitivität von Einzelangaben und der zur Deanonymisierung erforderliche Aufwand sind zu berücksichtigen. Anhaltspunkte können die Abschottungsmaßnahmen anläßlich der Volkszählung 1987 und die hierzu vorliegende Rechtsprechung bieten.

4. Bedienstete der Stadt-/Gemeindeverwaltung dürfen in einer abgeschotteten Stelle nur eingesetzt werden, wenn aufgrund ihrer bisherigen und zukünftigen beruflichen Tätigkeit oder aus anderen Gründen nicht zu besorgen ist, daß Erkenntnisse aus der Tätigkeit in der abgeschotteten Stelle zu Lasten von Auskunftspflichtigen oder sonst betroffenen Bürgern genutzt werden können.

5. Von zentraler Bedeutung ist die genaue Bestimmung der Abschottungsmaßnahmen in einer Dienstanweisung. Dies trägt dazu bei, daß der Bürger erkennen kann, unter welchen Bedingungen statistische Einzelangaben verarbeitet werden, insbesondere wie die erhobenen oder übermittelten Einzelangaben gesichert sind.

Regelungsbedürftig in einer Dienstanweisung sind aus der Sicht der Datenschutzkommission insbesondere folgende Punkte:

a) Organisatorische Zuordnung der abgeschotteten Stelle unmittelbar zum Oberbürgermeister/Bürgermeister; zwischengeschaltete Zuständigkeiten sind auf die Wahrnehmung der Dienstaufsicht zu beschränken.

b) Aufgabenbeschreibung der abgeschotteten Stelle (Durchführung bestimmter Bundes-, Landes- oder Kommunalstatistiken, Übernahme und Weiterverarbeitung von Einzelangaben aus bestimmten Bundes- oder Landesstatistiken); Zeitdauer der Einrichtung.

c) Benennung des Leiters der abgeschotteten Stelle und seiner Mitarbeiter (Anlage zur Dienstanweisung); Bestimmung der Funktionen und Verantwortlichkeiten.

d) Es sind nähere Bestimmungen bezüglich des Wechsels zwischen der Arbeit in der abgeschotteten Stelle und einem anderen Arbeitsplatz in der Verwaltung zu treffen. Hierbei sind der zu erwartende Geschäftsanfall, die Sensibilität der Daten und Gesichtspunkte der Praktikabilität zu berücksichtigen. Ein stundenweiser Wechsel sollte jedoch nur in Ausnahmefällen zugelassen werden (geringer Arbeitsanfall).

e) Verpflichtung auf das Statistik- und Datengeheimnis; Hinweis auf Folgen der Nichtbeachtung.

f) Genaue Bezeichnung der abzuschottenden Räume; Sicherungsmaßnahmen; Regelungen über die Zugangsberechtigungen; Verwehrung des Zutritts für Unbefugte; Überwachung.

g) Bestimmung der Arbeitszeit in der abgeschotteten Stelle; Bestimmung der Öffnungszeiten für den Publikumsverkehr (soweit erforderlich).

h) Anordnungen über den internen Postlauf.

i) Verbot der Anfertigung von Abschriften oder Vervielfältigungen für andere als Statistikzwecke sowie Durchführung von Rechtsbehelfs-, Vollstreckungs-, Bußgeld- oder Strafverfahren.

j) Löschung von Identifikatoren, die zur Aufgabenerfüllung nicht mehr erforderlich sind; Trennung von Erhebungs- und Hilfsmerkmalen.

6. Beim Vorliegen der formalen Voraussetzungen (Dateiverarbeitung, automatisiertes Verfahren) ist das Landesdatenschutzgesetz anzuwenden. Nach § 9 dieses Gesetztes i. V. m. der hierzu ergangenen Durchführungsverordnung vom 29. Dezember 1978, GVBl. S. 79, sind angemessene technische und organisatorische Maßnahmen zu treffen. Hinzuweisen ist ferner auf die Anmeldepflicht zum Datenschutzregister (§ 10) sowie auf die Kontrollbefugnisse der Datenschutzkommission. Die Sicherungsmaßnahmen müssen dem jeweiligen Stand der Technik entsprechen.

a) Für den Einsatz von Kleinrechenanlagen – PC – in den Erhebungsstellen bedeutet dies insbesondere:

- keine gleichzeitige Verwendung für Verwaltungsvollzugszwecke,

- Zugriffsschutz für Programme und Dateien, insbesondere
  Zugriffserlaubnis für definierte Benutzer,
  Zugriff nur auf definierte Daten,
  Zugriff nur auf definierte Programme bzw. Programmteile,

- Zugriffsschutz durch Paßwortsystem; Protokollierung von Benutzeraktivitäten, insbesondere von Kopiervorgängen,

- Online-Verschlüsselung der Festplatte, Kopierschutz durch Verschlüsselung,

- Ausschluß des Zugriffs zur Betriebssystemebene für Benutzer,

- Bootschutz vom Diskettenlaufwerk,

- Bestellung eines Systemverantwortlichen,

- Programmfreigabeverfahren und Programmdokumentation.

b) Sofern statistische Einzelangaben in Kommunalen Datenzentralen/Verwaltungsrechenzentren verarbeitet werden, sind die hierfür nach § 9 Landesdatenschutzgesetz erlassenen Dienstanweisungen Bestandteil der Abschottungsmaßnahmen. Zur Ergänzung des üblichen Datensicherungsstandards hält die Datenschutzkommission insbesondere folgende Maßnahmen für angemessen:

- Die unbefugte Eingabe von Daten sowie deren unbefugte Kenntnisnahme, Veränderung oder Löschung sind durch Datenverschlüsselung zu verhindern. In gleicher Weise sind Vorkehrungen gegen unbefugtes Ändern von Programmen zu treffen.

- Automatisierte Verarbeitungsvorgänge sind lückenlos zu protokollieren; die Protokolle sind für die Zeitdauer von fünf Jahren aufzubewahren.

- Bei Wegfall der Erforderlichkeit zur Aufgabenerfüllung der abgeschotteten Stellen, spätestens bei ihrer Auflösung, sind Datenträger mit Einzelangaben zu löschen. Die Löschung ist zu protokollieren. Auswertungs- und Zwischendateien sind zum frühestmöglichen Zeitpunkt zu löschen.