LANDTAG RHEINLAND-PFALZ
12. Wahlperiode

Drucksache 12/800
16. 12. 1991

126 Seiten

Unterrichtung

durch den Landesbeauftragten für den Datenschutz

Dreizehnter Tätigkeitsbericht nach § 21 des Landesdatenschutzgesetzes – LDatG – für die Zeit vom 1. Oktober 1989 bis 30. September 1991

Inhaltsverzeichnis

Dem Präsidenten des Landtags mit Schreiben vom 16. Dezember 1991 zugeleitet.

Druck: Landtag Rheinland-Pfalz, 20. Januar 1992

Abkürzungen:

AO	Abgabenordnung
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DOG	Dienstordnungsgesetz
Drs.	Drucksache
DSK	Datenschutzkommission

GG	Grundgesetz
HochschG	Landeshochschulgesetz
Kfz	Kraftfahrzeug
LDatG	Landesdatenschutzgesetz
LG	Landgericht
LfD	Landesbeauftagter für den Datenschutz
LKA	Landeskriminalamt
LKG	Landeskrankenhausgesetz
MG	Meldegesetz
MRRG	Melderechtsrahmengesetz
MS-DOS	Microsoft-Disk-Operating-System
NJW	Neue Juristische Wochenschrift
PC	Personal-Computer
PVG	Polizeiverwaltungsgesetz
Rdnr	Randnummer
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
Tb	Tätigkeitsbericht
TEMEX	Fernmeß- und Fernwirkdienst
Tz	Textziffer

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
12.	Tätigkeitsbericht Drs. 11/3427	v. 21. Dezember 1989

1 Vorbemerkung

1.1 Allgemeines

Gegen Ende der Elften Wahlperiode hat der Landesgesetzgeber den schon lange erwarteten Wechsel in der Organisation der Datenschutzkontrolle durch eine Änderung des Landesdatenschutzgesetzes (LDatG) vollzogen: An die Stelle der Datenschutzkommission als Kollegialorgan trat der Landesbeauftragte für den Datenschutz. Am 14. März 1991 hat der Landtag Rheinland-Pfalz mit Wirkung vom 15. April 1991 Dr. Walter Rudolf, Professor für Öffentliches Recht an der Universität Mainz, zum Landesbeauftragten für den Datenschutz gewählt.

Es war das Anliegen des Gesetzgebers, durch die Novellierung die Unabhängigkeit des Landesbeauftragten für den Datenschutz in Ausübung seines Amtes besonders hervorzuheben. Er hat die rechtliche Stellung einer unabhängigen obersten Landesbehörde und unterliegt keiner Dienst- und Rechtsaufsicht (§ 17 a LDatG). Diese gesetzgeberische Entscheidung bildet für den Amtsinhaber die wesentliche Arbeitsgrundlage, zugleich ist sie ihm auch Verpflichtung.

Der vorliegende, nach § 21 LDatG zu erstattende Tätigkeitsbericht ist – in Weiterführung der laufenden Zählung – der dreizehnte Bericht über die Datenschutz-Kontrollarbeit im Lande Rheinland-Pfalz. Da die Datenschutzkommission, deren Zusammensetzung sich seit dem 12. Tätigkeitsbericht nicht geändert hatte, darauf verzichtet hat, für die Zeit, in der ihre Kontrollzuständigkeit noch bestand – also vom 1. Oktober 1989 bis zum Amtsantritt des Landesbeauftragten für den Datenschutz am 15. April 1991 – einen Abschlußbericht vorzulegen, umfaßt dieser Bericht den gesamten zweijährigen Berichtszeitraum. Es wurde sorgfältig darauf geachtet, daß die jeweiligen Zuständigkeiten für Maßnahmen der Datenschutzkontrolle im Text erkennbar sind.

In der Weiterführung der Nummernfolge kommt aber auch zum Ausdruck, daß der Landesbeauftragte für den Datenschutz mit seiner Arbeit an die bewährte Tradition des Datenschutzes in Rheinland-Pfalz anknüpfen will. Es ist ihm insbesondere daran gelegen, die enge Anbindung der Datenschutzkontrolle an den Landtag zu erhalten und zu pflegen. Der Gesetzgeber hat hierfür mit der Beiordnung eines sechsköpfigen Beratungsgremiums, bestehend aus Parlamentariern und einem Vertreter der Landesregierung, gute Voraussetzungen geschaffen. In die Kommission beim Landesbeauftragten für den Datenschutz wurden berufen die Abgeordneten Franz Josef Bischel, Dieter Muscheid, Carsten Pörksen, Prof. Heinrich Reisinger und Leo Schönberg sowie der Staatssekretär im Ministerium des Innern und für Sport Klaus Rüter. Die Kommission konstituierte sich am 15. August 1991 und wählte den Abgeordneten Dieter Muscheid zum Vorsitzenden. Zum stellvertretenden Vorsitzenden wurde der Abgeordnete Franz Josef Bischel gewählt.

Dieser Tätigkeitsbericht wurde gem. § 18 a Abs. 3 Satz 4 LDatG in der Kommission vorberaten. Der Landesbeauftragte für den Datenschutz ist der Kommission für Anregungen und ihre Unterstützung dankbar.

Die organisatorische Anbindung der Behörde des Landesbeauftragten für den Datenschutz an den Landtag unterstreicht die Bedeutung, die der Gesetzgeber einer unabhängigen Datenschutzkontrolle beimißt.

Anläßlich der Wahl des Landesbeauftragten für den Datenschutz wurde die Arbeit der Datenschutzkommission noch einmal im Landtag gewürdigt. Besonders hervorgehoben wurde die intensive Beratungstätigkeit, die stets darauf gerichtet war, einen vernünftigen Ausgleich zwischen dem Interesse der Verwaltung an wirksamer Aufgabenerfüllung und dem Interesse der Bürger am Schutz ihrer Persönlichkeitsrechte zu finden. Auch der Landesbeauftragte für den Datenschutz sieht hier einen Schwerpunkt seiner Arbeit. Vorverlagerter Datenschutz durch Unterstützung der gesetzgeberischen Arbeit und die Beratung der Verwaltung in Datenschutzfragen leistet einen Beitrag zur Wahrung des Rechtsfriedens.

Datenschutz zielt nicht darauf, die Verwaltungsarbeit durch datenschutzrechtliche Vorschriften und Richtlinien zu erschweren. Es geht vielmehr darum, auf die rasante technische Entwicklung der Informationsverarbeitung zu reagieren und der Gefährdung von Persönlichkeitsrechten der Bürger entgegenzuwirken, die mit der Verarbeitung hochsensibler Daten, mit der Vernetzung von Datenverarbeitungssystemen und mit dem Einsatz von Arbeitsplatzrechnern einhergeht. Hierfür besteht, wie diesem Tätigkeitsbericht zu entnehmen ist, auch in Rheinland-Pfalz Handlungsbedarf.

Die Bürger des Landes müssen – wie in der Vergangenheit – darauf vertrauen können, in den Datenschutzkontrollorganen verläßliche Sachwalter ihrer Anliegen zu haben. Der Datenschutzkommission wurde gelegentlich das Lob ausgesprochen, schnell und „unbürokratisch" zu arbeiten. Der Landesbeauftragte für den Datenschutz wird alles daransetzen, die gute Tradition auch insoweit fortzuführen. Eingaben hilfe- und ratsuchender Bürger werden auch in der Zukunft mit Vorrang bearbeitet.

Dieser dreizehnte Tätigkeitsbericht ist recht umfangreich geworden. Der aufmerksame Leser wird bemerken, daß er sich nicht darauf beschränkt, die grundsätzlichen Fragen des Datenschutzes und die in der allgemeinen Diskussion befindlichen Probleme anzusprechen oder über grundlegende Kontroversen zwischen einzelnen Bereichen der Verwaltung und dem Datenschutz zu

informieren. Er enthält auch viele fallbezogene Darstellungen der täglichen Datenschutzarbeit. Da gerade diese Fallbeispiele dem Praktiker eine wertvolle Hilfe sein können, wurde darauf verzichtet, die Meßlatte der „Berichtswürdigkeit" höher zu legen.

Der Landesbeauftragte für den Datenschutz wird – wie in der Vergangenheit auch die Datenschutzkommission – immer wieder nach dem großen Datenschutzsündenfall oder gar Datenschutzskandal gefragt, dessen öffentliche Darstellung und Würdigung das Verständnis der Bevölkerung für die Notwendigkeit des Datenschutzes fördern könne. Vielleicht wird, wer diesen Tätigkeitsbericht in der Erwartung liest, über Skandale informiert zu werden, die Lektüre enttäuscht beenden. Aber ist es nicht aus der Sicht des Betroffenen ein ganz schwerwiegender, skandalöser Eingriff in seine Rechte, wenn er wiederholt vom Gerichtsvollzieher aufgesucht und durch Anschlag an die Haustür dessen gewaltsames Eindringen in die Wohnung angedroht wird, nur weil das Einwohnermeldeamt die Anschrift verwechselte? Ist es nicht auch aus der Sicht des Betroffenen ein Skandal und für eine rechtsstaatliche Verwaltung beschämend, wenn eine Führerscheinbehörde Vorgänge, die 17 bis 20 Jahre zurückliegen, zur Grundlage ihrer Entscheidung macht, obwohl diese Vorgänge schon längst aus der Führerscheinakte hätten entfernt werden müssen? Die Bewertung solcher Vorgänge hängt ganz wesentlich davon ab, aus welcher Sicht sie betrachtet werden. Die sachliche Darstellung in diesem Tätigkeitsbericht darf nicht darüber hinwegtäuschen, daß auch der Landesbeauftragte für den Datenschutz in vielen Fällen Eingaben in diesem Sinne bewertet.

1.2 Beteiligung des Landesbeauftragten für den Datenschutz an Vorgängen im Bereich der Landesregierung, die den Datenschutz betreffen

Eine wesentliche Voraussetzung für die Wahrnehmung der Beratungsaufgaben nach dem LDatG (§ 18 Abs. 1 Satz 2) ist die möglichst frühzeitige Unterrichtung über datenschutzrelevante Vorgänge der Staatskanzlei und der Ressorts. Schon im Jahre 1980 hatte deshalb die DSK die Landesregierung ersucht, ihr vor der Entscheidung in Datenschutzfragen von allgemeiner Bedeutung Gelegenheit zur Stellungnahme zu geben. Diesem Ersuchen wurde entsprochen: In der Staatskanzlei und in den Ministerien ergingen gleichlautende Verfügungen, die die Beteiligung der DSK an Vorgängen im Bereich der Landesregierung, die den Datenschutz betreffen, regelten. Es wurde insbesondere angeordnet, daß der DSK frühzeitig Gelegenheit zu geben ist, zu Gesetzentwürfen, Rechtsverordnungen und Verwaltungsvorschriften, die Bestimmungen über die Verarbeitung personenbezogener Daten enthalten, Stellung zu nehmen.

Die in dieser Weise inhaltlich bestimmte Zusammenarbeit war über lange Zeit zufriedenstellend. Bei einzelnen Ressorts geriet die erwähnte Verfügung allerdings in jüngerer Zeit in Vergessenheit. Bisweilen erhielt die DSK erst nach Information durch andere Datenschutzkontrollbehörden Kenntnis von datenschutzrelevanten Entwürfen, zu denen die Datenschutzbeauftragten des Bundes oder anderer Länder längst Stellung genommen hatten. Die Entwürfe wurden dann zwar auf Anforderung zur Verfügung gestellt, die für Stellungnahmen bestimmten Fristen waren aber abgelaufen.

Das Grundsatzproblem, daß eine Unterrichtung der DSK häufig dann unterblieb, wenn Rechts- und Verwaltungsvorschriften in Rede standen, die auf Bundesebene verabschiedet werden sollten, konnte in einem Schriftwechsel mit dem Ministerium des Innern einvernehmlich gelöst werden. In einem Schreiben vom 12. Februar 1987 teilte das Ministerium folgendes mit: „Nach Auffassung der Landesregierung bestehen allerdings keine Bedenken, über datenschutzrelevante Rechtsvorschriften und Verwaltungsbestimmungen des Bundes, die ihr zugeleitet werden, die DSK zu unterrichten. Voraussetzung ist allerdings, daß es sich hierbei nicht lediglich um ein internes Arbeitspapier, sondern um einen Entwurf handelt, der eine gewisse Verbindlichkeit hat und allgemein diskutiert wird. Eine Weiterleitung scheidet auch aus, wenn die zuständige Stelle des Bundes als Herr des Verfahrens Einwände gegen die Unterrichtung Dritter erhebt."

Der Bitte des LfD an die Landesregierung um Klarstellung, daß die Staatskanzlei und die Ressorts zukünftig auch mit der Behörde auf der Grundlage der obigen Anordnungen und Verfahrensregelungen zusammenarbeiten, wurde entsprochen. Der Chef der Staatskanzlei teilte mit, daß bei einer Erörterung der Angelegenheit in der Staatssekretärskonferenz volles Einvernehmen im Sinne des Anliegens des LfD festgestellt und beschlossen wurde, die Zusammenarbeit mit dem LfD zu verstärken. Zu diesem Zweck wurden unterdessen in der Staatskanzlei und in den Ressorts Koordinierungsreferenten bestellt.

1.3 Informations- und Bildungsarbeit

Der LfD sieht es als seine Aufbgabe an, das allgemeine Bewußtsein für den Datenschutz zu fördern. Darüber hinaus trägt er durch Informationen der verschiedensten Art dazu bei, die Kenntnisse über die Rechte und Pflichten aus dem Datenschutz als Teil des Persönlichkeitsrechts bei den Bürgern und in der Verwaltung zu erweitern und zu vertiefen. Dabei gilt es insbesondere, Antworten auf Fragen zu finden und zu vermitteln, die sich aus neuartigen Anforderungen der Praxis wie aus der fortschreitenden technischen Entwicklung ergeben.

Seit Jahren gab bereits die DSK in der Schriftenreihe „Informationen zum Datenschutz" allgemeine und bereichsspezifische Sammlungen von Gesetzestexten, Verordnungen und Verwaltungsvorschriften, ergänzt durch einschlägige Gerichtsentschei-

dungen sowie eigene Erläuterungen, heraus. Die große Nachfrage läßt darauf schließen, daß diese Veröffentlichungen als nützliche Arbeitshilfen angesehen werden. Bisher sind erschienen:

- Datenschutzrechtliche Vorschriften (Heft 1),
- Orientierungshilfe zu datenschutzrechtlichen Sicherungsmaßnahmen (Heft 2),
- Datenschutzrechtliche Anforderungen an wissenschaftliche Forschungsvorhaben (Heft 3),
- Datenschutz im Krankenhaus (Heft 4) und Datenschutz in der Gesundheitsverwaltung (Heft 5).

Die Mitarbeiter der Geschäftsstelle der DSK, jetzt der Behörde des LfD, übernehmen regelmäßig Referate im Rahmen der vom Ministerium des Innern und für Sport angebotenen informationstechnischen Grundbildung für Landesbedienstete.

Darüber hinaus werden auf Informationsveranstaltungen interessierter Fachkreise und -gruppen durch Referate und durch die Teilnahme an Diskussionen Grundlagen und Ziele des Datenschutzes mit besonderem Bezug auf die jeweils behandelten Bereiche vermittelt. Als Beispiele sind Zusammenkünfte der Datenschutzbeauftragten von Krankenhäusern, Richtern, Lehrern, Sozialarbeitern bei Gesundheitsämtern, Mitarbeitern von Kassenärztlichen Vereinigungen und von Sozialdiensten der Justiz zu nennen, aber auch einzelne Lehrveranstaltungen der Volkshochschulen.

Mit dem Fachbereich Informatik der Universität Kaiserslautern besteht seit einiger Zeit ein Austausch von Informationen und Meinungen, der fortgesetzt, intensiviert und auf Fachbereiche anderer Hochschulen, in denen Informatik zum Lehrangebot gehört, ausgeweitet werden soll. Im Rahmen der gegebenen materiellen Möglichkeiten wird der LfD hier jederzeit Hilfestellungen, sei es durch Bereitstellung von Informationsmaterial oder in sonstiger Weise, geben. Der LfD hält es für notwendig, daß in den Fachbereichen für Informatik der Hochschulen ständige Veranstaltungen über den Datenschutz im Lehrangebot vorgesehen werden.

Häufig wenden sich einzelne Bürger oder öffentlich Bedienstete an den LfD mit der Bitte um Zusendung von Informationsmaterial über den Datenschutz. Nicht selten handelt es sich dabei um Personen, die ihrerseits in ihrem jeweiligen Bereich Informationsveranstaltungen über den Datenschutz – zum Beispiel bei der Bereitschaftspolizei – durchführen. Ihnen wird nach Möglichkeit Material an die Hand gegeben, das nach ihren Wünschen auf ihre besonderen bereichsspezifischen Bedürfnisse und Fragestellungen zugeschnitten ist.

2 Anforderungen an das allgemeine Datenschutzrecht; Einschränkung der Datenschutzkontrolle durch den Bundesgesetzgeber (§ 24 Abs. 2 BDSG)

Nach § 24 Abs. 2 des neugefaßten Bundesdatenschutzgesetzes (BDSG) unterliegen personenbezogene Daten aus bestimmten Bereichen der Kontrolle des Bundesbeauftragten für den Datenschutz dann nicht, wenn der jeweils Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht. Dabei handelt es sich im wesentlichen neben dem Kontrollbereich der Kommission nach Art. 10 Grundgesetz um personenbezogene Daten, die dem Post- und Fernmeldegeheimnis und dem Arztgeheimnis unterliegen oder die sich in Personalakten oder in Akten über die Sicherheitsüberprüfung befinden. Die einzelne öffentliche Stelle unterrichtet – so regelt das BDSG weiter – unbeschadet des Kontrollrechts des Bundesbeauftragten für den Datenschutz die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht. Der für die Landesbeauftragten für den Datenschutz entscheidende Satz findet sich in Absatz 6 der genannten Bestimmung: Die Regelung gilt nämlich für die öffentlichen Stellen entsprechend, die für die Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

Die DSK hat bereits in einem frühen Stadium des Gesetzgebungsverfahrens in den Jahren 1988 und 1989 gegenüber dem Ministerium des Innern darauf hingewiesen, daß schon die Erstreckung der damals vorgesehenen Regelung auf die Datenschutzkontrolle nach Landesrecht auf verfassungsrechtliche Bedenken stößt. Auch der LfD kann keine Kompetenz des Bundesgesetzgebers zur Einschränkung der Kontrollbefugnisse der Landesdatenschutzbeauftragten erkennen. Es steht allein dem jeweiligen Gesetzgeber in den Ländern zu, die Kontrollaufgaben der Datenschutzbeauftragten festzulegen und abzugrenzen, während der Bund auf die Kompetenz zur Regelung der Kontrollaufgaben des Bundesbeauftragten für den Datenschutz beschränkt ist.

Unabhängig von der nicht von den Datenschutzbeauftragten verbindlich zu entscheidenden Frage einer Kompetenzüberschreitung kann es vorerst nur darum gehen, die Regelung im Sinne des allgemeinen Anliegens des Gesetzgebers in der Praxis so anzuwenden, daß datenschutzrechtliche Kontrollen in ihrer Effektivität so wenig wie möglich behindert werden. Massierte Widersprüche könnten sich z. B. bei systematischen Querschnittskontrollen auswirken, in denen zur Feststellung der verschiedenen Übermittlungswege von personenbezogenen Daten bestimmte miteinander im Zusammenhang stehende Reihen von Akten überprüft werden müssen. Bei den öffentlichen Stellen des Landes stimmt der Kreis der Betroffenen nach § 24 Abs. 2 Satz 4 Nr. 2 Buchst. c BDSG (Personalakten und Akten über die Sicherheitsüberprüfung) im wesentlichen überein mit den aktiven und ehemaligen Bediensteten sowie mit den Empfängern von Versorgungs- oder anderen Bezügen aus einem Beschäftigungsverhältnis. Auch im Falle des § 24 Abs. 2 Satz 4 Nr. 2 Buchst. b BDSG (Arztgeheimnis) beziehen sich die geschützten Daten häufig auf

öffentlich Bedienstete oder ihre Angehörigen (z. B. bei der Beihilfeberechnung berücksichtigungsfähige Personen). In besonderen Verwaltungsbereichen, wie etwa im Geltungsbereich des Sozialgesetzbuches oder der Prozeßordnungen, können auch andere Personen betroffen sein.

Darüber, wie das Widerspruchsrecht in der Praxis angewendet werden soll, insbesondere wie es den Betroffenen zur Kenntnis zu bringen ist, konnte mit dem Ministerium des Innern und für Sport Übereinstimmung erzielt werden. Kernpunkt ist die Feststellung, daß Kontrollen durch den LfD unabhängig vom Zeitpunkt der Unterrichtung der Betroffenen über ihr Widerspruchsrecht stattfinden können und demzufolge eine besondere Information über das Widerspruchsrecht vor angekündigten Kontrollen durch den LfD rechtlich nicht geboten ist. Der Unterrichtungspflicht nach § 24 Abs. 2 Satz 5 BDSG kann durch eine allgemeine Information (Hausmitteilung, Schwarzes Brett o. ä.) entsprochen werden. Ist der Kreis der Betroffenen größer, wählt die Behörde die zweckmäßigste Art der Unterrichtung.

Für die Zukunft wird eine Unterrichtung bei Beginn des Rechtsverhältnisses, aufgrund dessen personenbezogene Daten verarbeitet werden, empfohlen (z. B. beim Eintritt in das Beamtenverhältnis oder bei der Aufforderung, den Fragebogen für die Sicherheitsüberprüfung auszufüllen).

Das gewählte Verfahren ist praktikabel und auch angemessen, um das Widerspruchsrecht, das auch vom LfD bejaht wird, zu realisieren. Die Kontrolltätigkeit des LfD wird damit nicht in nennenswerter Weise behindert. Es wäre deshalb zu begrüßen, wenn sich die dem Anwendungsbereich des LDatG unterliegenden Behörden und sonstigen öffentlichen Stellen des Landes dem Vorgehen des Ministeriums des Innern und für Sport anschließen würden.

Das LDatG ist aus einer Reihe von Gründen novellierungsbedürftig. An dieser Stelle seien nur die wichtigsten kurz wiederholt (vgl. dazu ausführlich den 12. Tb der DSK, Tz.2.2, S.9 – 13):

- die personenbezogenen Daten, die in Akten gespeichert werden, sind – der bundesrechtlichen Regelung entsprechend – in den Geltungsbereich des Gesetzes einzubeziehen;
- die Phase der Datenerhebung muß im Datenschutzgesetz geregelt werden;
- die Transparenz behördlicher Datenverarbeitung muß durch weitere Informations- und Beteiligungsrechte der Bürger erhöht werden;
- die Zweckbindung muß auch gesetzlich als Grundsatz für den Umgang mit personenbezogenen Daten verankert werden;
- die Kontrollbefugnisse des LfD sollten präziser ausgestaltet werden;
- die neuen technischen Formen der Datenverarbeitung und Nutzung (TEMEX , Bildaufzeichnungstechniken) sollten gesetzlich beschränkt werden;
- generell ist eine Anpassung an das neue BDSG in Form und Inhalt (insbesondere auch bezogen auf die Verweisungen im LDatG auf das BDSG, s. dazu unten Tz. 17.1) erforderlich. Es ist zu erwarten, daß diese seit langem erhobenen Forderungen im nächsten Berichtszeitraum realisiert werden.

3 Die Situation des Datenschutzes in Europa

Die gegenwärtige Situation des Datenschutzes in Europa ist gekennzeichnet durch den dynamischen Fortschritt der Informationstechniken. Einerseits wird die Verarbeitung von Daten und insbesondere ihr Austausch beträchtlich erleichtert, andererseits sind die gesetzlichen Vorkehrungen zum Persönlichkeitsschutz in den einzelnen Mitgliedstaaten der EG sehr unterschiedlich entwickelt. In fünf der EG-Mitgliedstaaten fehlt es an Rechtsvorschriften zum Datenschutz. Wann diese erlassen werden, ist nicht abzusehen. Die Folgen sind unterschiedliche Rechtspositionen der Bürger mit Rückwirkungen auf die Wirtschaftsbedingungen in den Mitgliedstaaten.

Aus diesen Gründen hat das Europäische Parlament mit mehreren Entschließungen (1967, 1979 und 1982) die EG-Kommission aufgefordert, einen Richtlinienvorschlag für die dringend erforderliche Angleichung des Datenschutzes in den Mitgliedstaaten vorzulegen.

Nunmehr wird im Blick auf den unmittelbar bevorstehenden gemeinsamen Binnenmarkt die Dringlichkeit einer Harmonisierung des Datenschutzes in der EG vollends evident; denn dieser gemeinsame Binnenmarkt verstärkt den Austausch von Waren und Dienstleistungen und führt zu einem ständig anwachsenden Personenverkehr. Das Auftreten multinationaler Unternehmen und Berufsverbände aller Art wird zunehmen und eine erhebliche Ausweitung der Verarbeitung, insbesondere des Austausches personenbezogener Daten, wie z. B. Arbeitnehmerdaten, mit sich bringen.

Ein dichtes Netzwerk grenzüberschreitender Datenflüsse wird u. a. durch vermehrte Banküberweisungen, Flug-, Hotel- und sonstige Buchungen, aber auch durch die Tätigkeit von Auskunfteien, Werbeunternehmen und des Transportgewerbes entstehen. Hierzu werden auch Registergerichte, Gewerbeaufsichts-, Arbeits- sowie Finanzbehörden und nicht zuletzt das Meldewesen beitragen.

Unabhängig von der EG bestehen auf europäischer Ebene insbesondere zwei allgemeine Regelungen des Datenschutzes. An erster Stelle zu nennen ist das – bereits im 12. Tätigkeitsbericht der DSK erwähnte – Übereinkommen des Europarats vom 28. Januar 1981 zum Schutze der Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108), das leider inzwischen immer noch nicht von allen Mitgliedstaaten ratifiziert wurde. Wenn diese Konvention auch noch manche Option zur Umsetzung der von ihr definierten Rahmengrundsätze offen läßt, so hat sie sich doch über einen längeren Zeitraum als ein wirksames Instrument erwiesen und für die jetzt beabsichtigte europäische Kodifizierung allgemeinen Datenschutzrechts die wesentlichen Denkansätze geliefert.

Des weiteren ist in diesem Zusammenhang die Empfehlung des Rates der OECD vom 23. September 1980 von Bedeutung, die Leitlinien über den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr von personenbezogenen Daten enthält und zwar sowohl für den öffentlichen wie für den privaten Sektor. Auch die OECD hat damit eine wichtige Rolle für die Entwicklung des Datenschutzes übernommen.

So haben Japan und Australien Regelungen getroffen, die auf die OECD-Richtlinie zurückgehen. Die OECD bereitet gegenwärtig eine neue Richtlinie für die Sicherung der Informationssysteme vor, die im Januar 1992 vorgelegt werden soll.

Ein weiterer Vorschlag der Kommission der EG beinhaltet eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Kommunikationsnetzen. Mit dieser Richtlinie soll den Telekommunikationsnutzern insbesondere im dienstintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen ein Grundschutz garantiert werden. Die entsprechenden Forderungen wurden von den Datenschutzbeauftragten der Mitgliedstaaten bei ihrer Zusammenkunft in Berlin im August 1989 mit Nachdruck erhoben. Schon heute geht der Entwurf der Richtlinie zum Teil über das hinaus, was entsprechende Datenschutzregelungen der Bundesrepublik (TDSV und UDSV) dem betroffenen Bürger zugestehen.

Zu nennen sind ferner die bereits in Kraft getretene EG-Statistik-Verordnung, die Zusammenarbeit der Verwaltungsbehörden auf dem Gebiet der indirekten Besteuerung, die vom Ministerrat verabschiedete Richtlinie über den freien Zugang zu Informationen über die Umwelt sowie Fragen des Datenschutzes im Rahmen der Bestimmung des für die Prüfung von Asylanträgen zuständigen Mitgliedstaates.

Zur Zeit liegt der Entwurf der Kommission für eine Rahmenrichtlinie zur Angleichung bestimmter Rechts- und Verwaltungsvorschriften für den Datenschutz in den EG-Mitgliedstaaten – die sog. „Harmonisierungsrichtlinie" – zur Beratung dem Europäischen Parlament und dem Ministerrat vor. Diese Richtlinie verpflichtet die Mitgliedstaaten nur zu einem Mindeststandard, hindert also keinen Mitgliedstaat daran, in der Gewährung von Datenschutz weiterzugehen; sie wird auch Auswirkungen auf den Datenschutz in den deutschen Bundesländern haben. Der LfD wird daher in enger Zusammenarbeit mit seinen Kolleginnen und Kollegen den im Gange befindlichen Prozeß der Meinungs- und Willensbildung mit dem Ziel zu beeinflussen versuchen, einen höchstmöglichen Datenschutz zu erreichen. Auf der 13. Internationalen Konferenz der Datenschutzbeauftragten nahm die Behandlung der mit dem EG-Richtlinienentwurf zusammenhängenden Fragen einen breiten Raum ein. Die Basis für die Beurteilung des Entwurfs aus der Sicht des Datenschutzes in Deutschland bilden die Forderungen, die in einer Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes, der Länder und der DSK Rheinland-Pfalz vom 29. Januar 1991 enthalten sind (siehe Anlage 6). Dabei muß davon ausgegangen werden, daß die Bewertung der einzelnen Bestimmungen des Entwurfs nicht völlig isoliert aus dem Blickwinkel des verhältnismäßig hoch entwickelten deutschen Datenschutzrechts erfolgen kann.

Zumindest in folgenden Punkten entspricht der Richtlinienentwurf nicht den Erwartungen aus der Sicht des Datenschutzes:

- Das Konzept des Entwurfs beschränkt den Schutz personenbezogener Daten noch auf Dateien, eine Verkürzung, die auch im neuen BDSG aufgegeben wurde. Auch für die Mitgliedstaaten der EG muß der Schutz des Persönlichkeitsrechts für alle personenbezogenen Daten gelten.

- Das Prinzip der strikten Zweckbindung für die Verwendung und Weitergabe persönlicher Daten, wie es vom Bundesverfassungsgericht gefordert wird, muß auch EG-weit gelten.

- Die vorgesehenen Regelungen über die Auskunft an den Betroffenen – ein Kernstück des Datenschutzes und Voraussetzung für die Geltendmachung weiterer Rechte – bedarf der Verbesserung durch eine engere Begrenzung des Ausnahmekataloges; verbesserungsfähig ist der Entwurf auch hinsichtlich der Unterrichtung des Betroffenen bei der unmittelbaren Datenerhebung.

- Datenschutz hängt von der Unabhängigkeit der Kontrollbehörden ab. In dem Richtlinienentwurf wird das aber konsequent nur für die nationalen Kontrollbehörden, nicht aber auch für die EG anerkannt. Die Zusammensetzung der „Gruppe für den Schutz personenbezogener Daten" ist dieser Forderung anzupassen. Nicht der Vertreter der Kommission kann geborener

Vorsitzender sein. Der Vorsitzende ist von den Vertretern der nationalen Kontrollbehörden – Datenschutzbeauftragten – zu wählen.

- Die vorgeschlagenen Regelungen für den Datenexport in Drittländer bedürfen der Änderung. Es kann nicht sein Bewenden damit haben, als Voraussetzung in diesen Ländern ein „angemessenes" Schutzniveau zu fordern. Will man nicht zu dem grotesken Ergebnis gelangen, daß Datenübermittlungen in Drittländer geringeren rechtlichen Sicherungen unterliegen wie in EG-Partnerstaaten, kann die Voraussetzung nur ein gleichwertiges Schutzniveau sein.

- Nicht zuletzt ist es geboten, Überlegungen darüber anzustellen, wie ein gleichwertiger Datenschutz auch im privaten Sektor erreicht werden kann. Dies müßte durch bereichsspezifische Regelungen realisiert werden. Auch in diesem Punkt entspricht der Entwurf nicht den aus der Sicht des Datenschutzes gestellten Erwartungen.

Die Kommission hat bereits in einer Empfehlung vom 29. Juli 1981 (ABL der EG Nr. 246 v. 29. August 1981, S. 31) hervorgehoben, daß der Schutz personenbezogener Daten den Charakter eines Grundrechts habe. Der endgültige Regelungsgehalt der Richtlinie sollte dieser Erkenntnis Rechnung tragen und damit einen entscheidenden Beitrag zu dem viel genannten und allseits gewünschten „Europa der Bürger" bilden.

4 Meldewesen

4.1 Neukonzeption des Einwohnerinformationssystems

Das Einwohnerinformationssystem, abgekürzt EWOIS, wird seit dem Jahre 1971 betrieben. Es bildet die funktionale Grundlage für die Automatisierung des Einwohnermeldewesens und der damit zusammenhängenden einwohnerbezogenen Aufgabenerfüllung. Kernbestandteile sind eine Datenbank, in der die Meldedaten aller Einwohner des Landes gespeichert sind, und ein zentral gesteuertes, flächendeckendes Datenkommunikationsnetz.

EWOIS beruht auf einem Programmsystem, das in seinen Grundzügen vor dem Jahr 1971 entwickelt und in der Folgezeit mit erheblichem Aufwand ergänzt und den veränderten Anforderungen angepaßt wurde. Die Komplexität des Programmsystems und seine geringe Strukturtransparenz erschweren es zunehmend, notwendige Verbesserungen mit angemessenem Aufwand zu realisieren, den Wünschen der Meldebehörden, die Auftraggeber des Verfahrens sind, bezüglich der Entwicklung neuer Anwendungen innerhalb des Systems zu entsprechen und EWOIS so zu organisieren, daß den Datenschutzanforderungen des Meldegesetzes in vollem Umfange entsprochen ist. Die verfahrensmäßigen Umstellungen aufgrund der Bestimmungen des Meldegesetzes über die Löschung und Aufbewahrung von Daten (§ 5) beispielsweise wurden aus den genannten Gründen immer wieder aufgeschoben. Die Gesellschaft „Kommunale Datenverarbeitung Rheinland-Pfalz GmbH" (KDV GmbH), der die Betreuung, Pflege und Weiterentwicklung des Verfahrens übertragen wurde (vgl. 12. Tb., Tz. 16.4), teilte mit, daß „auch die programmtechnischen Gegebenheiten (Programmiersprache und Datenbanksystem), die auf einem zwischenzeitlich veralteten technischen Stand sind, die Wartung des Verfahrens nicht nur erschweren, sondern in absehbarer Zeit unmöglich machen".

Die KDV GmbH wurde vom Ministerium des Innern und für Sport beauftragt, eine Projektstudie für ein EWOIS auf neuer programmtechnischer Grundlage zu erarbeiten. Diese soll notwendige Änderungen beschreiben, Kostenschätzungen enthalten und zeitliche Vorgaben für die Realisierung nennen. Zur Unterstützung der KDV GmbH wurde eine Projektgruppe gebildet, in der in Wahrnehmung des gesetzlichen Beratungsauftrags auch Vertreter der Behörde des LfD mitarbeiten.

Der LfD begrüßt es, daß eine Neuentwicklung von EWOIS auch dazu genutzt werden soll, Datenschutzdefizite zu beheben. Diesbezügliche Anforderungen wurden dem Ministerium bereits in einem Schreiben der DSK vom September 1990 mitgeteilt. Er meint aber auch, daß den auf eine Neuentwicklung von EWOIS gerichteten Überlegungen eine politische Grundsatzentscheidung vorausgehen müßte, die Entscheidung nämlich, ob ein landeseinheitliches Verfahren, so wie es durch § 37 Meldegesetz vorgezeichnet ist, auf Dauer beibehalten werden soll. Vor zwei Jahrzehnten war es angesichts der damals verfügbaren Datenverarbeitungstechnik sicherlich notwendig, die Rationalisierung des Meldewesens durch die Zentralisierung der Datenverarbeitung anzustreben. Heute sind indessen ganz andere Lösungsansätze denkbar und möglich. In Betracht käme beispielsweise eine verteilte Datenverarbeitung oder eine automatisierte Registerführung vor Ort, wobei es die Aufgabe des Landesrechenzentrums sein könnte, den überregionalen Zugriff, soweit er in Ausnahmefällen aufgrund gesetzlicher Regelung beibehalten werden kann, sicherzustellen. Da mit diesen Organisationsfragen auch Datenschutzprobleme angesprochen sind, erscheint es angezeigt, diese Gesichtspunkte in die Diskussion um eine Reform des Meldewesens in Rheinland-Pfalz einzubringen.

4.2 Novellierung des Melderechtsrahmengesetzes

Ein bereits in der vergangenen Wahlperiode von der Bundesregierung eingebrachter Gesetzentwurf zur Änderung des Melderechtsrahmengesetzes (Bundestagsdrucksache 11/5111) konnte vom Deutschen Bundestag in zweiter und dritter Lesung nicht

mehr behandelt werden, so daß er der Diskontinuität zum Opfer fiel. Zu diesem Gesetzentwurf hatten eine Reihe von Datenschutzbeauftragten und auch die DSK Stellung genommen und Änderungen und Ergänzungen angeregt, die das informationelle Selbstbestimmungsrecht der Bürger stärker zur Geltung bringen sollten.

Ein vom Bundesminister des Innern ausgearbeiteter Referentenentwurf, der dem LfD vom Ministerium des Innern und für Sport zur Stellungnahme vorgelegt wurde, knüpfte an die Vorarbeiten in der 11. Wahlperiode des Deutschen Bundestages an. Leider wurden einzelne Verbesserungen, die als Ergebnisse der Beratungen des Innenausschusses des Deutschen Bundestages bereits Eingang in dessen Beschlußempfehlung gefunden hatten (Bundestagsdrucksache 11/8310), nicht übernommen. So soll nach dem Referentenentwurf die sog. Hotelmeldepflicht beibehalten werden, obwohl bereits der Innenausschuß die Streichung empfohlen hatte; sie betrifft die Verpflichtung „beherbergter Personen", besondere Meldevordrucke handschriftlich auszufüllen und die Verpflichtung des „Leiters der Beherbungsstätte", diese Vordrucke zur Einsichtnahme oder Abholung bereitzuhalten.

Von den Datenschutzbeauftragten des Bundes und der Länder wird die Forderung nach Streichung der gesetzlichen Regelungen über die Hotelmeldepflicht schon seit Jahren erhoben. Es wird darauf verwiesen, daß die allgemeine Meldepflicht bezweckt, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Erledigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotelmeldepflicht nicht in die Systematik des Melderechts; es handelt sich vielmehr um materielles Polizeirecht.

Die DSK unterstützte die Forderung nach Wegfall der Hotelmeldepflicht, nahm aber bezüglich der Frage, ob auch die sog. Krankenhausmeldepflicht – sie verpflichtet zur Bereithaltung von Patientenlisten durch die Krankenhausverwaltung für polizeiliche Zwecke – entfallen sollte, eine abweichende Haltung ein. Zwar paßt auch die Krankenhausmeldepflicht – ebenso wie die Hotelmeldepflicht – aus den oben angegebenen Gründen nicht in die Systematik des Melderechts; es darf indessen nicht übersehen werden, daß sie im Bereich der Strafverfolgung ein außerordentlich wichtiges Korrektiv zu den sehr weitgehenden Regelungen zum Schutze des Patientengeheimnisses darstellt. Ärzte und sonstige Bedienstete von Krankenhäusern (Krankenschwestern, Krankenpfleger, Verwaltungspersonal) haben strafprozessuale Zeugnisverweigerungsrechte, die nur bei prozeßrechtlich wirksamer Entbindung von der Schweigepflicht entfallen (§ 53, 53 a StPO). Im übrigen besteht – soweit das Zeugnisverweigerungsrecht reicht – eine Verschwiegenheitspflicht für Ärzte und Berufshelfer in Ermittlungsverfahren, die nur beim Vorliegen der allgemeinen Rechtfertigungsgründe durchbrochen werden kann. Vor dem Hintergrund dieser Gesetzeslage besteht selbst dann, wenn schwerwiegende Straftaten aufzuklären sind, für die Polizei keine Informationsmöglichkeit, wenn sie nicht nach Melderecht die Befugnis hätte, die für diesen Zweck geführten Aufzeichnungen einzusehen. Schließlich ist auch zu berücksichtigen, daß schon nach geltendem Melderecht eine regelmäßige Übermittlung der Krankenhausmeldungen an die Polizei unzulässig ist. Die Polizei ist damit grundsätzlich gehindert, die Eintragungen außerhalb der Wahrnehmung gesetzlicher Befugnisse im Einzelfall zur Kenntnis zu nehmen. Die Regelung der Krankenhausmeldepflicht im Meldegesetz entspricht nach Auffassung des LfD dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz.

Der LfD begrüßt die Regelung in dem Referentenentwurf, die die Krankenhausmeldepflicht im Grundsatz beibehält, zugleich aber die Verwendung der Daten konkretisiert: Ihre Nutzung soll nur zur Abwehr einer erheblichen Gefahr, zur Verfolgung von Straftaten oder zur Aufklärung des Schicksals von Vermißten und Unfallopfern im Einzelfall zugelassen sein.

Ergänzungsbedürftig sind nach Meinung des LfD die Bestimmungen über die regelmäßige Datenübermittlung. Er hält es für geboten, die Datenübermittlung beim Vorliegen einer Auskunftssperre wegen Adoptionspflege in näher bestimmten Fällen auszuschließen.

Mit der Einführung eines Widerspruchsrechts gegen die Erteilung von Melderegisterauskünften an Parteien und Wählergruppen für Wahlwerbezwecke wird einer von der Datenschutzseite seit langem erhobenen Forderung entsprochen. Die damit verbundene Stärkung des informationellen Selbstbestimmungsrechts der Bürger ist geeignet, Verärgerungen, wie sie beispielsweise durch die Wahlwerbung der DVU im Zusammenhang mit der Europawahl entstanden sind, zu begegnen.

4.3 Auslegungsfragen im Melderecht

Der Klärungsbedarf bezüglich datenschutzrechtlicher Fragen nimmt ab, je länger sich ein Gesetz in Geltung befindet. Die Vielzahl von Stellungnahmen zu konkreten Fragen des Datenschutzes im Meldewesen im Verlauf einer fast zehnjährigen Geltungsdauer des Meldegesetzes ermöglicht es, Anfragen oft sehr schnell auf der Grundlage früherer Beratungen der DSK und von Abstimmungen mit dem Ministerium des Innern und für Sport zu beantworten. Dennoch gibt es gelegentlich auch neue Probleme, für die Lösungen erarbeitet werden müssen. Dies muß im Bereich des Meldewesens mit besonderer Sorgfalt geschehen, denn die Stellungnahmen beziehen sich häufig auf allgemein eingeführte Verfahrensweisen und haben deshalb eine weit über den Einzelfall hinausgehende Wirkung.

Vor diesem Hintergrund haben auch die folgenden Fragen besonderes Gewicht:

4.3.1 Meldedatenübermittlung an Religionsgemeinschaften

Es war zu klären, ob bei der in § 32 Abs. 1 Nr. 11 Meldegesetz vorgesehenen Übermittlung der Zahl der minderjährigen Kinder an öffentlich-rechtliche Religionsgemeinschaften auch die Zahl derjenigen Kinder, die einer anderen Religionsgemeinschaft angehören oder bei denen der Übermittlung von Meldedaten gemäß § 32 Abs. 2 Satz 2 Meldegesetz widersprochen wurde, mitgeteilt werden darf. Ferner baten die Vertreter der Religionsgemeinschaften, ihnen auch Übermittlungssperren bei einem konfessionsverschiedenen Kind bzw. konfessionsverschiedenen Ehegatten mitzuteilen. Ein Erfordernis hierfür wurde damit begründet, daß durch die Kenntnis von Übermittlungssperren viele unnötige Ermittlungen und Rückfragen vermieden werden könnten.

Die DSK erhob keine Bedenken gegen die Übermittlung der Anzahl aller minderjährigen Kinder eines Betroffenen, auch wenn Übermittlungssperren gem. § 32 Nr. 2 Satz 2 Meldegesetz vorliegen. Dabei ging sie davon aus, daß die Übermittlung der Gesamtzahl der minderjährigen Kinder in erster Linie ein personenbezogenes Datum der Eltern darstellt.

Auch gegen die Bekanntgabe von Übermittlungssperren an öffentlich-rechtliche Religionsgesellschaften erhob sie keine Einwendungen, sofern lediglich die Existenz des Widerspruchs eines Familienangehörigen mitgeteilt wird und die Angabe anderer Daten, die zu einer Identifizierung des Widersprechenden beitragen könnten, unterbleibt.

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

In ihrem 12. Tätigkeitsbericht schilderte die DSK unter Tz. 4.4 ihre Bemühungen, den Schutz des Adoptionsgeheimnisses bei der Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgesellschaften zu verbessern. Mit ihrer Initiative reagierte die DSK auf Vorgänge, in denen die bevorstehende Adoption dadurch gefährdet worden war, daß die Pflegekinder unter ihrem Geburtsnamen, den sie bis zur Adoption tragen, angeschrieben worden waren. Auch der Hinweis auf die in das Melderegister eingetragene Übermittlungssperre konnte – wie die Erfahrungen zeigten – nicht sicherstellen, daß Daten, die durch das Adoptionsgeheimnis geschützt sind, durch Initiativen der Kirchengemeinden ungewollt Unbefugten offenbart wurden.

Da nach Auffassung der DSK besondere Gründe des öffentlichen Interesses im Sinne des § 1758 BGB die Übermittlungen an die Religionsgesellschaften nicht rechtfertigen können, wurden Bedenken gegen diese Übermittlungspraxis gegenüber dem Ministerium des Innern geäußert. Dieses konnte sich den Bedenken jedoch nicht anschließen. Es sah § 32 des Meldegesetzes als vorrangige Rechtsvorschrift gegenüber § 1758 BGB an und folgerte hieraus, daß es auf besondere Gründe des öffentlichen Interesses nicht ankommen könne. Da § 32 des Meldegesetzes der Regelung des § 19 des Melderechtsrahmengesetzes entspräche, seien verfassungsrechtliche Bedenken hinsichtlich einer Aushöhlung des Adoptionsgeheimnisses durch den Landesgesetzgeber nicht begründet.

Die Evangelische Kirche begründete ihr Interesse an den Daten von Kindern in Adoptionspflegeverhältnissen mit der Notwendigkeit, den urkundlichen Nachweis der Taufe als konstitutives Tatbestandsmerkmal der Kirchenmitgliedschaft uneingeschränkt erbringen zu können. Außerdem würden die Daten zur Berichtigung der Kirchenbücher benötigt.

Die Katholische Kirche vertrat gegenüber dem ISM den Standpunkt, daß die Nichtübermittlung der Daten gerade nicht geeignet sei, das Adoptionsgeheimnis in der erforderlichen Weise zu schützen. Wenn das zuständige Pfarramt keine Kenntnis von einem bestehenden Adoptionspflegeverhältnis habe, sei die Möglichkeit nicht auszuschließen, daß bei der Anmeldung zu kirchlichen Amtshandlungen, bei denen auf das Taufbuch zurückgegriffen werden müsse, unklare und für alle Beteiligten überraschende Situationen entstünden. Das scheinbar unrichtige Taufbuch zwinge den Pfarrer, Nachfragen anzustellen und um Klarstellungen zu bitten. Dies könne die Adoptivpflegeeltern in eine Erklärungsnot bringen, die das Zustimmungserfordernis des § 1758 Abs. 1 BGB überspiele und dem besonderen öffentlichen Interesse an der Geheimhaltung des Adoptionspflegeverhältnisses zuwiderlaufe. Im übrigen trage die Übermittlung dazu bei, daß die in den Pfarrämtern geführten Personenstandsbücher richtig und die Eintragungen zweifelsfrei seien. Dies liege auch im öffentlichen Interesse, weil die kirchlichen Bücher in bestimmten Fällen subsidiär an die Stelle staatlicher Nachweise treten könnten.

Der LfD strebt eine Lösung an, wie sie in Bayern gefunden wurde. § 13 Abs. 1 der Bayer. Meldedatenübermittlungsverordnung sieht vor, daß eine Datenübermittlung u. a. an öffentlich-rechtliche Religionsgesellschaften dann zu unterbleiben hat, wenn im Melderegister eine Auskunftssperre wegen Adoptionspflege gespeichert ist. Bei der Novellierung der Meldedatenübermittlungsverordnung, die auch aus anderen Gründen geboten ist (vgl. Tz. 4.7), wird der LfD entsprechende Vorschläge machen.

4.3.3 Staatsangehörigkeit adoptierter Kinder

Nach § 96 des novellierten Ausländergesetzes (AuslG) erhalten jugendliche Ausländer, die sich rechtmäßig im Bundesgebiet

aufhalten, eine Aufenthaltsgenehmigung, wenn diese bis zum 31. Dezember 1991 beantragt wird. Die Landesbeauftragte für Ausländerfragen unterrichtete die Eltern der Betroffenen durch persönlich adressierte Schreiben über die Antragsbefugnis und den Fristablauf. Für die Adressierung wurden Daten des Melderegisters verwendet.

In einer größeren Zahl von Fällen wurden auch die Adoptiveltern solcher Kinder angeschrieben, die vor der Adoption zwar Ausländer waren, durch die Adoption aber nach § 6 RuStAG die deutsche Staatsangehörigkeit erworben hatten. Diese Kinder waren als Deutsche durch § 96 AuslG nicht betroffen; die oben erwähnte Unterrichtung war demzufolge nicht nur entbehrlich, sondern begründete bei den Adoptiveltern auch die Besorgnis, daß das Adoptionsgeheimnis gefährdet sei.

Örtliche Feststellungen durch einen Mitarbeiter des LfD in vier Einwohnermeldeämtern ergaben folgendes:
Die adoptierten Kinder waren mit ihrem durch die Adoption erworbenen Namen im Melderegister eingetragen, es fehlte indessen der Hinweis auf ihre deutsche Staatsangehörigkeit. Die Eintragung der durch die Adoption erworbenen deutschen Staatsangehörigkeit könne – so die Auskunft der Meldeamtssachbearbeiter – erst erfolgen, wenn die Geburt und die Adoption vom Standesbeamten des Standesamtes I in Berlin beurkundet und der Meldebehörde eine Mitteilung nach § 300 Abs. 3 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden zugegangen sei. In zwei Fällen konnte diese Mitteilung schon deshalb nicht erfolgt sein, weil es das örtliche Standesamt, das vom Vormundschaftsgericht nach Nr. XIV MiZi über die Annahme des Kindes unterrichtet wurde, unterlassen hatte, beim Standesamt I in Berlin das Verfahren nach § 41 PStG auf Anordnung zur Beurkundung der Geburt eines außerhalb des Geltungsbereichs des Personenstandsgesetzes geborenen Kindes einzuleiten.

Es kann nach Auffassung des LfD für die Eintragung der deutschen Staatsangehörigkeit in das Melderegister auf die Mitteilung des Standesamtes I Berlin nicht ankommen, denn die Adoptiveltern hatten bei der Anmeldung der Kinder zum Melderegister entweder die Adoptionsurkunde vorgelegt oder andere Nachweise erbracht, denen die Meldebehörde entnehmen konnte, daß ein Kind mit ausländischer Staatsangehörigkeit, aber dem Familiennamen der Adoptiveltern, deren Haushalt angehört. Im erstgenannten Falle ist die deutsche Staatsangehörigkeit nachgewiesen, im zweiten Falle hat die Meldebehörde den Sachverhalt von Amts wegen zu ermitteln (§ 24 VwVfG). In jedem Falle müßten die Bemühungen der Meldebehörden darauf gerichtet sein, das Melderegister in den Fällen, in denen die deutsche Staatsangehörigkeit von Adoptivkindern nicht eingetragen ist, nach § 10 MG von Amts wegen zu berichtigen oder zu ergänzen. Das Ministerium des Innern und für Sport wurde um Mitteilung gebeten, in welcher Weise die Unrichtigkeiten des Melderegisters am zweckmäßigsten zu beheben sind. Eine Stellungnahme lag zum Zeitpunkt der Abfassung dieses Berichtsbeitrags noch nicht vor.

4.3.4 Weitergabe von Gesamteinwohnerlisten an Ortsbürgermeister

An die zuständigen Aufsichtsbehörden wie auch an die DSK wurde wiederholt die Frage herangetragen, ob es rechtlich zulässig ist, Ortsbürgermeistern Gesamteinwohnerlisten zur Erfüllung ihrer Aufgaben zur Verfügung zu stellen.

Eine ausdrückliche gesetzliche Regelung dieser Datenweitergabe enthalten weder das Meldegesetz noch die Meldedaten-Übermittlungsverordnung. § 8 dieser Verordnung sieht eine regelmäßige Datenübermittlung und Datenweitergabe lediglich für die Zwecke der Ehrung von Alters- und Ehejubilaren und zur Erfüllung der Aufgaben der Ortsgemeinden im Zusammenhang mit der Anmeldung eines Einwohners vor. In diesen Fällen dürfen die in dieser Vorschrift genannten Daten über den jeweiligen Betroffenen mitgeteilt werden. Eine regelmäßige Überlassung von Gesamteinwohnerlisten an Ortsbürgermeister kann auf § 8 indessen nicht gestützt werden.

Es bestehen allerdings keine Bedenken, einem Ortsbürgermeister auf Anforderung im Einzelfall nach § 31 Abs. 1 Meldegesetz eine Einwohnerbestandsliste mit den Vor- und Familiennamen, etwaigen akademischen Graden und der Anschrift der Einwohner zu überlassen. Auch wenn die Übermittlung nur zur Information des Ortsbürgermeisters über die in seiner Ortsgemeinde lebenden Einwohner dient, ist eine Unterrichtung auf der Grundlage der genannten Vorschrift zulässig. Ein anderes Ergebnis wäre auch kaum zu vertreten angesichts der sonstigen vom Meldegesetz zugelassenen Datenübermittlungen. Auskünfte, die den Namen, akademische Grade und die Anschrift enthalten, dürfen nach § 34 Abs. 1 Meldegesetz an jedermann erteilt werden, ohne daß hierfür ein berechtigtes Interesse dargelegt werden müßte, und auch die entsprechende Datenweitergabe an Adreßbuchverlage ist nach § 35 Abs. 4 zulässig, soweit nicht der Betroffene Widerspruch hiergegen eingelegt hat.

Zu der Gesamtproblematik hatte die DSK bereits in ihrem 8. Tätigkeitsbericht unter Tz. 3.2 Buchst. c Stellung genommen und darauf hingewiesen, daß kein Hinderungsgrund besteht, Ortsbürgermeistern Meldedaten in einem für die Aufgabenerfüllung erforderlichen Umfange zu übermitteln. Als Aufgaben, zu deren Erfüllung die Daten benötigt werden können, sind die Durchführung von Informationsveranstaltungen, die Versendung von Informationsschriften und die Vorbereitung von Altennachmittagen genannt worden.

Im Ergebnis ist also die Überlassung einer Gesamteinwohnerliste mit den oben genannten Daten auf Anforderung eines Orts-

bürgermeisters nach § 31 Abs. 1 MG zulässig. Eine derartige Liste kann von dem Ortsbürgermeister aufgrund der regelmäßigen Übermittlung von Meldedaten nach § 8 der Meldedaten-Übermittlungsverordnung ergänzt und fortgeschrieben werden. Selbstverständlich ist bei der Verwendung der übermittelten Daten das Zweckbindungsgebot des Meldegesetzes zu beachten.

4.3.5 Auskünfte über Alters- und Ehejubiläen

An die Meldebehörden wird von Mitgliedern des Deutschen Bundestags und des Landtags immer wieder der Wunsch herangetragen, periodisch Daten über Alters- und Ehejubiläen mitzuteilen. Das Ministerium des Innern und für Sport hatte nach Abstimmung mit den Melderechtsreferenten anderer Länder zunächst den Standpunkt vertreten, als besondere Form der Gruppenauskunft unterliege die Weitergabe von Daten über Alters- und Ehejubiläen auch den Übermittlungsrestriktionen für Gruppenauskünfte. Dies bedeute, daß eine periodische Auskunftserteilung, die materiell einer regelmäßigen Datenübermittlung gleichkomme, melderechtlich unzulässig sei.

Gelegentlich einer erneuten Erörterung dieser Frage im Berichtszeitraum ließ das Ministerium indessen erkennen, daß es die folgende Praxis nach der Gesetzeslage für zulässig hält: Es kann auf Antrag eine periodische Übermittlung für die Gesamtzeitdauer eines Jahres erfolgen; die im einzelnen stattfindenden Übermittlungen sind indessen wegen des nach § 35 Abs. 3 bestehenden Widerspruchsrechts auf solche Jubiläen zu beschränken, die innerhalb eines Zeitraumes von zwei Monaten nach der Auskunftserteilung stattfinden.

Die DSK hielt diese Änderung des Auskunftsverfahrens nach der bestehenden Gesetzeslage für zulässig.

4.3.6 Erteilung von Gruppenauskünften aus dem Melderegister

Dem LfD gehen immer wieder Bürgereingaben und Anfragen von Behörden zu, die die Erteilung von Gruppenauskünften aus dem Melderegister zum Gegenstand haben. Gruppenauskünfte unterscheiden sich von Einzelauskünften dadurch, daß Informationen nicht bezüglich einer bestimmten, namentlich bezeichneten oder in anderer Weise individualisierten Person begehrt werden, sondern das Auskunftsinteresse auf solche – bisher unbekannte – Personen gerichtet ist, die einer durch ein bestimmtes Merkmal gekennzeichneten Gruppe angehören (beisp. Gruppe der Fünfzigjährigen, Gruppe mit gleichem Geschlecht, Gruppe mit gleichem Familienstand). § 34 Abs. 3 des Meldegesetzes läßt die Erteilung einer Gruppenauskunft zu, wenn diese Auskunft im öffentlichen Interesse liegt.

Im Berichtszeitraum wurde u. a. die Frage akut, ob es zulässig ist, Gruppenauskünfte an den Vermieter (Eigentümer eines Mietshauses, dessen Bevollmächtigten oder dgl.) über die für bestimmte Gebäude im Melderegister verzeichneten Personen zu geben. Von Datenschutzseite wurde gegen die Erteilung einer Gruppenauskunft eingewandt, daß es um rein kommerzielle Interessen gehe, die zwar möglicherweise ein berechtigtes Interesse als Voraussetzung einer Einzelauskunft, nicht aber ein öffentliches Interesse als Voraussetzung einer Gruppenauskunft begründen könnten. Von seiten der Fachbehörden wurde argumentiert, das öffentliche Interesse könne sich aus dem Interesse der Allgemeinheit an der Richtigkeit des Melderegisters ergeben. Die Auskunft an den Vermieter käme der Richtigkeit des Melderegisters zugute, weil der Vermieter nach Erhalt der Auskunft notwendige Melderegisterberichtigungen entweder von sich aus mitteile oder entsprechende Rückmeldungen zur Unrichtigkeit einer Melderegistereintragung auf Verlangen der Meldebehörde vorzunehmen habe.

Die DSK vertrat die Auffassung, daß die Erteilung einer Gruppenauskunft aus dem Melderegister an Vermieter durchaus in Betracht kommen könne. Sie hielt es für zulässig, vom Vorliegen der gesetzlichen Voraussetzung, nämlich eines öffentlichen Interesses, auszugehen, wenn es dem Vermieter nur aufgrund einer Gruppenauskunft möglich ist, Rechtsansprüche gegenüber den Bewohnern oder ehemaligen Bewohnern geltend zu machen. Ferner hielt sie es in analoger Anwendung von Rechtsgrundsätzen des Verwaltungsverfahrensrechts für naheliegend, davon auszugehen, daß der Wohnungsgeber als Beteiligter am Verwaltungsverfahren beim Vorliegen der Voraussetzungen des § 29 VwVfG ein Informationsrecht hat.

Vom Amt für Einwohnerwesen einer größeren Stadt wurden Bedenken bezüglich der Erteilung einer Gruppenauskunft an ein Markt- und Meinungsforschungsinstitut geltend gemacht. Für eine Befragung zum Einkaufsverhalten und zur Werbewirksamkeit von Zeitungsanzeigen war um Übermittlung einer Stichprobenauswahl von rund 1 000 Adressen gebeten worden. Im Blick auf den kommerziellen Hintergrund der Befragungsaktion war es durchaus verständlich, daß das Vorliegen der Übermittlungsvoraussetzung – öffentliches Interesse – in Zweifel gezogen wurde.

Es ist freilich auch zu berücksichtigen, daß es wohl gerade in der Absicht des Gesetzgebers lag, mit der Vorschrift über die Erteilung von Gruppenauskünften eine Rechtsgrundlage für die Übermittlung von Meldedaten an Markt- und Meinungsforschungsinstitute zu schaffen. Die Kommentare sowohl zum Melderechtsrahmengesetz (Medert/Süßmuth, Rdnr. 48 zu § 21) wie auch zum Meldegesetz Rheinland-Pfalz (Weiler/Demare, Erläuterungen zu § 34 Abs. 3) nennen Markt- und Meinungsforschungsinstitute ausdrücklich als Übermittlungsempfänger, unterlassen dabei aber jegliche Differenzierung nach Art und Inhalt der Befragungen, die von diesen Instituten durchgeführt werden.

Der LfD geht davon aus, daß die Gruppenauskunft zulässig ist, auch wenn es sich um Befragungen der in Rede stehenden Art handelt. Zwar ist der gesetzgeberische Wille, durch Verwendung des unbestimmten Rechtsbegriffs „öffentliches Interesse" nur undeutlich zum Ausdruck gebracht. Das öffentliche Interesse besteht aber insoweit, als die Tätigkeit von Markt- und Meinungsforschungsinstituten dazu beiträgt, Marktgeschehen transparent zu machen und den Markt funktionsfähig zu halten.

Wenn der Gesetzgeber zuläßt, daß das Melderegister die Datenbasis für Stadtadreßbücher bildet, ist es wohl nicht angemessen, an die Erteilung einer Gruppenauskunft zum Zwecke der Zusendung von Befragungsunterlagen einen strengeren Maßstab anzulegen. Es ist jedoch zu berücksichtigen, daß schutzwürdige Belange Betroffener nicht beeinträchtigt werden.

Von Bedeutung ist in diesem Zusammenhang auch, daß den Betroffenen durch § 34 Abs. 6 MG die Möglichkeit eingeräumt ist, die Melderegistereintragung für Gruppenauskünfte sperren zu lassen, wenn sie der Auffassung sind, durch die Einbeziehung in Befragungen von Markt- und Meinungsforschungsinstituten in ihren schutzwürdigen Belangen beeinträchtigt zu sein.

Zusammenfassend vertritt der LfD die Auffassung, daß datenschutzrechtliche Gesichtspunkte einer Erteilung von Gruppenauskünften in den dargestellten Fällen nicht entgegenstehen.

4.4 Übermittlung von Meldedaten an die Kfz-Zulassungsstellen

§ 5 der Meldedatenübermittlungsverordnung läßt zur Erfüllung von Aufgaben der Kreisverwaltungen als Kraftfahrzeugzulassungsstellen die Übermittlung bestimmter Grunddaten aus dem Melderegister im Online-Verfahren zu. Die DSK stellte fest, daß dieser Online-Zugriff nicht nur auf die Meldedaten des regionalen Zuständigkeitsbereichs der Kraftfahrzeugzulassungsstellen, sondern landesweit eröffnet wurde.

Sie beurteilte die Zulässigkeit der überregionalen Meldedatenübermittlung wie folgt: In der Meldedatenübermittlungsverordnung ist nicht geregelt, in welchem Umfang die Befugnis zum Zugriff auf Meldedaten besteht. Zwar ist die Art der Daten, auf die zugegriffen werden darf, enumerativ aufgezählt. Eine Regelung der regionalen Komponente ist jedoch unterblieben. Diese Frage ist also durch Interpretation der gesetzlichen Vorschriften zu klären. Dabei ist maßgeblich auf die Verordnungsermächtigung in § 31 Abs. 5 Satz 3 Meldegesetz abzustellen. Nach dieser Vorschrift darf ein automatisiertes Übermittlungsverfahren nur dann eingerichtet werden, soweit die zum Abruf bereitgehaltenen Daten ihrer Art nach für den Empfänger erforderlich sind und das Bereithalten der Daten zum sofortigen Abruf durch den Empfänger unter Berücksichtigung der schutzwürdigen Belange des Betroffenen angemessen ist. Die Verordnungsermächtigung betont also den Erforderlichkeitsgrundsatz sowie die Verpflichtung zur Wahrung schutzwürdiger Belange der Betroffenen.

Es ist ferner zu berücksichtigen, daß Normadressat melderechtlicher Vorschriften die jeweils regional zuständige Meldebehörde ist, die demzufolge im Grundsatz nur eine Befugnis zur Übermittlung von Meldedaten aus ihrem räumlichen Zuständigkeitsbereich haben kann.

Die DSK kam zu dem Ergebnis, daß der landesweite Zugriff auf Meldedaten vom Gesetzgeber als Regelfall nicht gewollt und – auch unter Berücksichtigung der vom Ministerium des Innern und für Sport sowie vom Ministerium für Wirtschaft und Verkehr hierfür vorgetragenen Gründe – nicht erforderlich ist. Sie forderte, die Zugriffsmöglichkeiten der Kraftfahrzeugzulassungsstellen der Kreisverwaltung auf die Meldedaten solcher Einwohner zu begrenzen, die ihren Wohnsitz im jeweiligen Zuständigkeitsbereich dieser Behörden haben.

Das Ministerium des Innern und für Sport wies das Landesrechenzentrum Ende 1989 an, die Zugriffsmöglichkeiten der Zulassungsstellen entsprechend zu beschränken. Dies ist mit fast zweijähriger Verzögerung im August 1991 geschehen.

4.5 Mitwirkungspflicht des Wohnungsgebers im Meldeverfahren

Zwar ist häufig die Rede vom Vertrauensverhältnis zwischen dem Bürger und der öffentlichen Verwaltung, tatsächlich aber sind Gesetze und Verordnungen gespickt mit Bestimmungen, die keinem anderen Zweck dienen als dem, die Vollständigkeit und Richtigkeit von Angaben zu kontrollieren. So auch das Meldegesetz: § 14 verpflichtet den Wohnungsgeber, bei der An- und Abmeldung mitzuwirken. Der Wohnungsgeber oder sein Beauftragter hat dem Meldepflichtigen den Einzug und den Auszug schriftlich zu bestätigen; diese Bestätigung ist der Meldebehörde vorzulegen.

In einem der DSK durch eine Eingabe bekanntgewordenen Fall konnte die Bestätigung des Wohnungsgebers wegen dessen vorübergehender Abwesenheit nicht bei der Anmeldung vorgelegt werden. Daraufhin veranlaßte die Meldebehörde den Meldepflichtigen, ersatzweise den mit dem Wohnungsgeber abgeschlossenen Mietvertrag beizubringen, fertigte hiervon eine Ablichtung und nahm diese zu den Meldeakten.

Die Substituierung der Mitwirkung des Wohnungsgebers durch die erzwungene Vorlage des Mietvertrages ist nicht zulässig. Das datenschutzrechtliche Problem besteht darin, daß die Meldebehörde auf diese Weise erheblich mehr Informationen zur Kenntnis nimmt, als der Bestätigung des Wohnungsgebers bei Verwendung des hierfür vorgesehenen Vordruckes zu entnehmen sind. Soweit die fristgemäße Vorlage der Bestätigung des Wohnungsgebers wegen einer längeren Abwesenheit des Vermieters nicht möglich ist, wird dem Meldepflichtigen eine angemessene Fristverlängerung einzuräumen sein.

Der geschilderte Vorgang steht zugleich als Beispiel für eine Verwaltungsübung, die leider immer mehr um sich greift: die geradezu exzessive Kopiersucht. Hierauf hat schon die DSK hingewiesen (vgl. 11. Tb., Tz. 12.4.3) und auch in völliger Übereinstimmung mit dem Rechnungshof klargestellt, daß es in den meisten Fällen durchaus genügt, den prüfungsfähigen Nachweis für eine entscheidungserhebliche Tatsache durch einen kurzen Vermerk zu führen.

Hätte im obigen Fall der Meldepflichtige, weil der Wohnungsgeber vorübergehend nicht erreichbar war, aus eigenem Antrieb den Mietvertrag als Beweismittel vorgelegt und hätte der Meldeamtssachbearbeiter vermerkt, daß die Richtigkeit der Meldeangaben durch den Mietvertrag nachgewiesen ist, wäre gegen eine solche Verfahrensweise nicht das geringste einzuwenden.

4.6 Namensverwechslungen

Namensverwechslungen bei der Erteilung von Melderegisterauskünften sind nach wie vor ein ernstes Problem sowohl für die Betroffenen wie auch für die Empfänger einer unrichtigen Auskunft. Schon in ihrem 11. Tätigkeitsbericht hatte die DSK über Einzelfälle berichtet und die Forderung erhoben, daß Behörden bei Auskunftsersuchen grundsätzlich das in aller Regel bekannte Geburtsdatum zum Zwecke der eindeutigen Identifizierung des Gesuchten angeben und daß das Geburtsdatum von den Meldebehörden bei Recherchen im Melderegister verwendet wird (vgl. Tz. 6.1.2). Sie hatte den Meldebehörden ferner empfohlen, nicht zuletzt zur Vermeidung schwerwiegender haftungsrechtlicher Folgen, Anfragen von Personen oder Stellen, die das Geburtsdatum nicht angeben können, mit einem Vorbehalt bezüglich des verbliebenen Identifizierungsrisikos zu versehen. Eine weitere Empfehlung war darauf gerichtet, dieses Verfahren programmtechnisch in der Weise zu unterstützen, daß bei Auskünften aufgrund von Melderegisterrecherchen ohne Verwendung des Geburtsdatums der empfohlene Hinweis automatisch ausgedruckt wird.

Den Anliegen der DSK wurde beim Erlaß von Verwaltungsvorschriften zur Durchführung des Meldegesetzes teilweise entsprochen. Tz. 28.1 bestimmt, daß Melderegisterauskünfte, bei denen die Anfragenden das Geburtsdatum des Betroffenen nicht angeben können und dessen Identität auch im übrigen nicht eindeutig festgestellt werden kann, mit einem entsprechenden Vorbehalt zu versehen sind. Die auf eine programmtechnische Unterstützung des Auskunftsverfahrens gerichtete Empfehlung wurde, soweit bekannt, nicht aufgegriffen.

Die Hinweise der DSK und die Maßnahmen der obersten Aufsichtsbehörde konnten indessen noch keine hinreichende Sensibilisierung der Meldebehörden für das Problem bewirken: Nach wie vor bilden Namensverwechslungen bei Melderegisterauskünften einen Schwerpunkt bei Eingaben an die Behörde des LfD.

Welch schlimme Folgen aus Nachlässigkeiten bei der Erteilung von Melderegisterauskünften erwachsen können, zeigt folgender Fall: Ein junger Mann mit einem nicht gerade seltenen und daher sehr verwechslungsanfälligen Namen hatte einen Namensvetter, der laut Melderegister früher in der gleichen Straße, aber unter einer anderen Hausnummer, wohnte. Mit diesem Namensvetter wurde er bei Melderegisterauskünften verwechselt, obwohl er inzwischen auch selbst den Wohnsitz gewechselt hatte. Die Verwechslung hatte zur Folge, daß gegen ihn mehrere Vollstreckungsmaßnahmen eingeleitet wurden und sogar ein Haftbefehl erging. Recherchen der DSK ergaben, daß der Betroffene auch im Schuldnerverzeichnis und mit seiner aktuellen Anschrift bei der Schufa mit entsprechenden Negativmerkmalen gespeichert war. Ob und inwieweit bei Empfängern des Schuldnerverzeichnisses, wie z. B. Industrie- und Handelskammern und Kreditschutzorganisationen, ebenfalls unzutreffende Angaben gespeichert und von diesen an Dritte übermittelt worden waren, konnte nicht geklärt werden.

Für die Fehler bei der Auskunftserteilung gab es mehrere Ursachen: Sie entstanden zum einen dadurch, daß die in § 11 Meldegesetz normierte Pflicht zur Löschung und gesonderten Aufbewahrung inaktueller Meldedaten nebst den gesetzlichen Verwendungsbeschränkungen selbst acht Jahre nach dem Inkrafttreten des Meldegesetzes noch nicht realisiert ist. Würden inaktuelle Meldedaten nach § 11 Meldegesetz gelöscht und gesperrt, hätte die frühere Anschrift des Betroffenen, die zu der Verwechslung führte, nicht für die Recherche genutzt werden können.

Im konkreten Falle erklärte das Ministerium des Innern und für Sport seine Bereitschaft, einer Löschung der früheren Anschrift des Betroffenen im Melderegister zuzustimmen. Die frühere Anschrift steht damit für Recherchen im automatisierten Verfahren nicht mehr zur Verfügung; das Verwechslungsproblem ist damit wohl dauerhaft gelöst.

Generell ist zu beklagen, daß die Meldebehörden das Geburtsdatum nicht in der gebotenen Weise bei der Melderegisterrecherche als Identifikationsmerkmal verwenden. Würden sie dies tun, würden Verwechslungen in den meisten Fällen erkannt.

Sofern das Geburtsdatum von der anfragenden Stelle nicht benannt werden kann, muß die Melderegisterauskunft verweigert oder zumindest mit einem Vorbehalt versehen werden.

Die DSK erhob gegenüber dem Ministerium des Innern und für Sport ferner die Forderung, umgehend die Protokollierung der Abfragen aus EWOIS einschließlich der Kennung des abfragenden Bediensteten vorzunehmen, da nur dann die Realisierung von Ansprüchen der durch fehlerhafte Auskünfte Geschädigten aussichtsreich erscheint. Außerdem forderte sie, daß für einen gewissen Zeitraum auch festgehalten wird, an wen die Auskunft erteilt wurde.

Das Ministerium will darauf hinwirken, daß Meldeamtssachbearbeiter in geeigneter Weise auf die Verwechslungsgefahr hingewiesen werden. Den gesetzlichen Bestimmungen bezüglich der Löschung und Verwendungsbeschränkung inaktueller Meldedaten könne, so das Ministerium, nur im Rahmen einer völligen Neuentwicklung des EWOIS-Verfahrens entsprochen werden. „Spätestens im Zuge dieser angestrebten Verfahrensneuentwicklung", so teilte es mit, „ist auch beabsichtigt, die bestehenden melderechtlichen Anforderungen zu realisieren".

4.7 Regelmäßige Meldedatenübermittlung an die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ)

Die GEZ, die mehr als 26 Mio. Teilnehmerkonten führt, ist bestrebt, diese auf einem aktuellen Stand zu halten. Dies geschieht noch überwiegend durch formulargestützte Einzelauskünfte aus den Melderegistern (ca. 450 000 Einzelauskünfte jährlich im Bundesgebiet).

Sie ist bemüht, den Zeit-, Verwaltungs- und Kostenaufwand durch die Einführung neuer technischer Verfahren zu reduzieren. Gedacht ist an ein „Datenträgeraustauschverfahren für Einzelauskünfte". Das technische Konzept sieht, soweit bekannt, vor, daß dem Landesrechenzentrum ein Magnetband zur Verfügung gestellt würde, das Anschriften enthält, die nach den Erkenntnissen der GEZ inaktuell sind. Diese Anschriften sollen im automatisierten Verfahren mit dem Melderegister abgeglichen und aktualisiert werden. Angeblich wird dieses Verfahren in den Städten Berlin, Kiel, München und Stuttgart bereits erfolgreich praktiziert.

Der LfD hält das Verfahren für förderungswürdig, denn es würde eine erhebliche Rationalisierung der Verwaltungsarbeit bewirken. In der Stadt Mainz beispielsweise würden jährlich 4 000 bis 5 000 Einzelauskünfte entbehrlich. Zugleich ist er der Meinung, daß zusätzliche Datenschutzrisiken durch angemessene technische und organisatorische Datenschutzmaßnahmen auszuschließen sind.

Einer raschen Realisierung des Datenabgleichs stehen indessen gesetzliche Restriktionen entgegen. Ein auf unbestimmte Zeitdauer wiederholt stattfindender automatisierter Datenabgleich ist als „regelmäßige Datenübermittlung" zu qualifizieren. Regelmäßig sind Datenübermittlungen, „die aufgrund einer vorherigen Entscheidung in allgemein bestimmten Fällen stattfinden, ohne daß über die Datenübermittlung im konkreten Einzelfall nochmals entschieden wird" (so die Begründung zum Gesetzentwurf der Landesregierung). Eine regelmäßige Datenübermittlung an öffentliche Stellen – wie die GEZ – ist nach § 31 Abs. 4 Meldegesetz nur zulässig, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist. Die Verordnungsermächtigung in Absatz 5 verpflichtet den Minister des Innern und für Sport, in der Rechtsverordnung Anlaß und Zweck der Übermittlung, die Datenempfänger, die zu übermittelnden Daten sowie das Nähere über Form und Verfahren der Übermittlung zu bestimmen. Die auf der Grundlage dieser Ermächtigung erlassene Meldedatenübermittlungsverordnung enthält keine Bestimmungen über den automatisierten Abgleich von Meldedaten und Daten der GEZ. Schon aus diesem formalen Grunde kann das Verfahren daher z. Z. nicht praktiziert werden. Unter materiellen Gesichtspunkten ist von Bedeutung, daß die Zulässigkeitsvoraussetzungen der Datenübermittlung bei regelmäßigen Datenübermittlungen für alle folgenden Übermittlungsfälle zunächst abstrakt festgelegt und im Einzelfall dann nur noch einmal daraufhin überprüft werden müssen, ob sie diesen einmal getroffenen Festlegungen entsprechen (vgl. Medert/Süßmuth, Kommentar zum MRRG, Rdnr. 55 zu § 18). Zugleich muß die Erforderlichkeitsprüfung im Einzelfall durch eine abstrakt-generelle Entscheidung ersetzt werden. Dies ist grundsätzlich dem Gesetz- bzw. Verordnungsgeber vorbehalten.

Die rheinland-pfälzische Meldedatenübermittlungsverordnung aus dem Jahre 1984 ist auch aus anderen Gründen dringend überarbeitungs- und ergänzungsbedürftig. Die Novellierung sollte nicht zuletzt im Blick auf die Lösung von Problemen der geschilderten Art bald in Angriff genommen werden.

4.8 Übernahme von Meldeaufgaben durch die Ausländerbehörde

In einer ausführlichen Stellungnahme äußerte sich die DSK zu Überlegungen einer größeren Stadt, im Interesse einer rationellen Aufgabenerfüllung und der Bürgerfreundlichkeit melderechtliche Aufgaben für Ausländer durch die Ausländerbehörde wahrnehmen zu lassen. Konkret war beabsichtigt, daß An- und Abmeldungen von der Ausländerbehörde entgegengenommen und

dem Einwohnermeldeamt zur Erfassung im automatisierten Verfahren zugeleitet werden.

Die DSK verwies auf die Verpflichtung der Verwaltung, der Gefahr einer Verletzung des Persönlichkeitsrechts (Recht auf informationelle Selbstbestimmung) durch organisatorische und verfahrenssichernde Vorkehrungen entgegenzuwirken (BVerfG 65/1): Aus der Einheit der Gemeindeverwaltung folgt keine informationelle Einheit; der Grundsatz der informationellen Gewaltenteilung gilt auch innerhalb der Gemeindeverwaltung (BVerfG 1. BvR 962/87).

Eine Zusammenfassung von Behörden, die entsprechend ihrer Funktion organisatorisch getrennt sind, würde – so die DSK – der Verpflichtung zum Persönlichkeitsschutz durch verfahrenssichernde Maßnahmen zuwiderlaufen. Es müsse verhindert werden, daß Interessenkonflikte eintreten, die zu unzulässigen Eingriffen in das Recht auf informationelle Selbstbestimmung führen. Dem Meldeamt und der Ausländerbehörde stünden zur Erfüllung ihrer jeweiligen Aufgaben unterschiedliche Daten von Ausländern zur Verfügung, auf die die jeweils andere Behörde grundsätzlich nicht zugreifen dürfe.

Die DSK verkannte indessen nicht, daß auch die auf eine Konzentration der Aufgabenwahrnehmung gerichteten Bestrebungen der Verwirklichung eines bedeutsamen Anliegens der öffentlichen Verwaltung dienen: Bürgerfreundlichkeit und Verwaltungsvereinfachung sind Gesichtspunkte, die auch vor dem Hintergrund der datenschutzrechtlichen Überlegungen ein eigenständiges Gewicht haben und angemessen zu berücksichtigen sind. Folgende Lösungen könnten in Betracht gezogen werden:

- Es könnte daran gedacht werden, eine „Außenstelle" des Meldeamtes räumlich in das Ausländeramt zu inkorporieren. Zu diesem Zweck könnte etwa ein Mitarbeiter des Meldeamtes während der Dienststunden, in denen das Ausländeramt für Publikumsverkehr geöffnet ist, Aufgaben des Meldeamtes in den Räumen der Ausländerbehörde wahrnehmen. Es würde aus datenschutzrechtlicher Sicht dann auch nichts dagegen sprechen, diesen Bediensteten mit den erforderlichen Hilfsmitteln (EWOIS-Terminal) auszurüsten, wobei dabei selbstverständlich die üblichen Datensicherungsstandards zu beachten wären.

- Falls dies aus Gründen des Personalaufwands o. ä. nicht möglich ist, wäre auch (in Anlehnung an Modelle anderer Bundesländer, die sog. Bürgerbüros oder Bürgerämter eingerichtet haben) daran zu denken, der Ausländerbehörde die Möglichkeit einzuräumen, die Meldevordrucke an die in Betracht kommenden Ausländer auszuhändigen und ausgefüllte Vordrucke entgegenzunehmen. Dabei müßten jedoch folgende Vorgaben beachtet werden:
  Für die betroffenen Ausländer darf es keinen Zwang geben, sich der Mithilfe des Ausländeramtes bei der Wahrnehmung ihrer Anmeldepflichten zu bedienen. Es muß ihnen freigestellt bleiben, die Meldevorgänge auch beim Meldeamt abzuwikkeln. Außerdem ist darauf hinzuweisen, daß die Ausländerbehörde keine Doppel der Meldevorgänge in den Ausländerakten aufbewahren und auch sonstige Informationen aus dem Meldevorgang nicht speichern darf, die ihr aufgrund ihrer ausländerpolizeilichen Tätigkeit nicht zugänglich wären. Unter diesen Voraussetzungen spricht auch nichts dagegen, eine Vorprüfung bzw. Beratung derjenigen Ausländer in bezug auf Melderechtsfragen zuzulassen, die von diesem Angebot Gebrauch machen. Dabei ist es unbedenklich, wenn die Ausländerpolizei auch die EWOIS-Daten nutzt, die ihr zu ausländerpolizeilichen Zwecken bereits zur Verfügung stehen.

5 Polizei

5.1 Rechtsverordnungen zur Informationsverarbeitung nach dem Polizeiverwaltungsgesetz

Durch das Vierte Landesgesetz zur Änderung des Polizeiverwaltungsgesetzes wurden die Bestimmungen über die Informationsverarbeitung (§§ 25 a bis 25 g) eingefügt, um die Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zu ziehen. In drei Fällen enthalten diese Bestimmungen die Ermächtigung zum Erlaß von Rechtsverordnungen, für die nunmehr Entwürfe des Ministeriums des Innern und für Sport vorliegen. Bei ihrer Erarbeitung wurde der LfD beteiligt.

Im ersten Fall geht es um die regelmäßige Informationsübermittlung durch die Polizei in Fällen, in denen personenbezogene Daten durch den Einsatz besonderer technischer Mittel verdeckt erhoben wurden (§ 25 a Abs. 2 Satz 2), oder in bestimmten gesetzlich vorgesehenen Fällen, wenn die Polizei öffentlich nicht zugängliche personenbezogene Informationen durch die genannten Mittel oder Personen erhoben hat (§ 25 b). Sollen derartige Informationen regelmäßig übermittelt werden, bedarf es hierzu nach § 25 c Abs. 5 einer Rechtsverordnung des Ministers des Innern und für Sport, in der der Zweck der Übermittlung, die Informationsempfänger, die zu übermittelnden Informationen sowie das Nähere über Form und Verfahren der Übermittlung bestimmt werden.

Durch die Verordnung sollen regelmäßige Übermittlungen nur an Polizeibehörden zugelassen werden, nicht hingegen auch an andere öffentliche und nichtöffentliche Stellen. Es ist aus der Sicht des Datenschutzes zu begrüßen, daß von der auch insoweit vorhandenen gesetzlichen Ermächtigung kein Gebrauch gemacht worden ist. Eine Ausnahme hiervon ist die in § 5 zugelassene regelmäßige Übermittlung an die Nachrichtendienste und an die Sicherheitsorgane der Stationierungsstreitkräfte. Die DSK hatte vorgeschlagen, die im Gesetz geregelten differenzierten Voraussetzungen für die Datenerhebung, die auch für die regel-

mäßige Übermittlung gelten, in der Verordnung zu wiederholen oder wenigstens auf sie ausdrücklich Bezug zu nehmen, wodurch Irrtümer in der Praxis von vornherein ausgeschlossen worden wären. Der Anregung ist jedoch nicht gefolgt worden. Übernommen wurde hingegen der vorgeschlagene Hinweis zu § 2 Abs. 1, daß Direktabrufverfahren unter Verordnungsvorbehalt stehen. Ebenfalls auf einen Vorschlag der DSK geht die in § 2 Abs. 4 vorgesehene Nachberichtspflicht zurück. Stellt sich heraus, daß personenbezogene Daten, die nach dieser Verordnung übermittelt wurden, unvollständig oder unrichtig sind, müssen sie gegenüber dem Empfänger unverzüglich berichtigt werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

Die DSK hatte auch – wie es der Wortlaut der Verordnungsermächtigung vorsieht – gefordert, die zu übermittelnden Informationen zu bestimmen, also im einzelnen festzulegen, welche personenbezogenen Informationen übermittelt werden dürfen. Auch dies wurde nicht akzeptiert. Es ist zwar einzuräumen, daß die Polizei aufgrund ihrer allgemeinen Verpflichtung zur Gefahrenabwehr – wenn überhaupt – nur schwer auf einen abschließend festgelegten Katalog von Einzeldaten beschränkt werden kann. Dem Ziel des Gesetzes, mehr Transparenz zu schaffen, hätte es aber bereits gedient, wenn die bisher aus der polizeilichen Arbeit bekannten wesentlichen Gruppen von Daten genannt worden wären und dem Bedürfnis, unvorhersehbar notwendige regelmäßige Übermittlungen nicht auszuschließen, durch die Voranstellung des Wortes „insbesondere" entsprochen worden wäre. Die zusammenfassende Nennung in dem Generalbegriff „zu übermittelnde Informationen" wird dem Willen des Gesetzgebers in diesem Zusammenhang sicher am wenigsten gerecht.

Mit dem Entwurf einer Verordnung der Landesregierung „zur regelmäßigen Überprüfung von Dateien der Polizei, die zu Zwecken der Gefahrenabwehr errichtet worden sind", sollen gem. § 25 e Abs.1 die zeitlichen Abstände festgelegt werden, in denen polizeiliche Dateien auf ihre Erforderlichkeit hin zu überprüfen sind. Der festgelegte Abstand von fünf Jahren erscheint auch aus der Sicht des Datenschutzes als angemessen. Zu begrüßen wäre allerdings – wie von der DSK vorgeschlagen – ein Hinweis gewesen, daß die Möglichkeit einer früheren Überprüfung oder Löschung einer Datei durch die Festlegung der Fünfjahresfrist nicht ausgeschlossen ist.

Der Entwurf einer weiteren Verordnung des Ministers des Innern und für Sport betrifft „die Anordnung der Errichtung automatisierter Dateien der Polizei zur Gefahrenabwehr" (§ 25 g Abs. 2). Den im Gesetz vorgeschriebenen Errichtungsanordnungen kommt aus der Sicht des Datenschutzes eine erhebliche Bedeutung zu, denn sie ermöglichen in jedem einzelnen Fall spezifische datenschutzrechtliche Festlegungen. Wegen der in § 10 Abs. 2 geregelten Anmeldepflicht kann der LfD dabei jeweils vor Errichtung der Datei seiner Beratungspflicht gezielt nachkommen. Die Zusammenfassung der Zuständigkeit zur Errichtung beim Ministerium des Innern und für Sport erleichtert die Abstimmung über datenschutzrechtliche Notwendigkeiten und ist zu begrüßen. Zur Zeit sieht der Entwurf für die speichernde Stelle bei dem Antrag an das Ministerium eine Frist von sechs Wochen vor der ersten Speicherung vor. Da im LDatG der gleiche Zeitraum als Frist für die Anmeldung durch das Ministerium beim LfD vorgesehen ist, wäre für die erstgenannte Frist ein angemessen längerer Zeitraum zweckentsprechend gewesen.

5.2 Rückmeldungen der Justiz im polizeilichen Informationssystem

Die Rückmeldungen der Justiz an die polizeilichen Ermittlungsstellen über den Ausgang strafgerichtlicher Verfahren haben große Bedeutung bei der Verwirklichung des Rechts auf informationelle Selbstbestimmung. Aus Anlaß der Rückmeldung wird die im Zuge polizeilicher Ermittlungen vorgenommene Speicherung im Polizeilichen Informationssystem aktualisiert bzw. gelöscht. Wenn dies nicht geschieht, kann der Betroffene jederzeit mit dem alten Verdacht konfrontiert werden, wie er sich aus den nicht aktualisierten Vorgängen ergibt. Angesichts der Wichtigkeit dieser Rückmeldungen und ihrer Umsetzung im Polizeilichen Informationssystem ist eine jeweils schnelle, präzise und gewissenhafte Erledigung in besonderem Maße geboten.

Durch eine Eingabe wurde der DSK bekannt, daß die Umsetzung der Rückmeldungen in der Praxis noch nicht den erforderlichen Grad an Zuverlässigkeit aufweist, der notwendig ist, um die Betroffenen vor Nachteilen zu schützen.

Der Beschwerdeführer war von seiner geschiedenen Ehefrau wegen versuchten Totschlags angezeigt worden. Nach einer Verurteilung in erster Instanz wurde er im Berufungsverfahren freigesprochen. Die in Nr. 11 MiStra vorgeschriebene Rückmeldung der zuständigen Justizbehörde erging wenige Wochen darauf an die speichernde Polizeibehörde, die Kriminalinspektion einer Kreisverwaltung, wo die Löschung der Daten aus heute nicht mehr feststellbaren Gründen unterblieb. Als der Beschwerdeführer etwa zwei Jahre später bei einer Behörde eine gesetzlich vorgeschriebene Erlaubnis beantragte, vor deren Erteilung die Zuverlässigkeit des Antragstellers geprüft werden muß, stellte sich heraus, daß über ihn noch Informationen über das Ermittlungsverfahren unter der Tatbezeichnung „versuchter Totschlag" gespeichert waren.

Die DSK hat die unterbliebene Löschung der belastenden Daten gegenüber dem Ministerium des Innern und für Sport als einen erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen gewertet.

Die Kriminalinspektion veranlaßte die gebotene Löschung und nahm den Vorgang zum Anlaß, im Rahmen des Dienstunterrichts auf die Beachtung der einschlägigen datenschutzrechtlichen Bestimmungen hinzuweisen.

5.3 Namensnennung von Zeugen in Verwarnungsgeldverfahren

Bei Verwarnungsgeldangeboten ist es weithin üblich, daß die Bußgeldstellen in den Schreiben an die Betroffenen Namen und Anschrift der Anzeigeerstatter nennen, wie dies auch in Bußgeldbescheiden geschieht. Nicht selten handelt es sich um Parkverstöße, durch die – beispielsweise durch Zuparken einer sog. „Kannlinie" – Geschäftsinhaber in nicht unerheblicher Weise beeinträchtigt werden. Die Folge sind dann bisweilen Belästigungen der Anzeigenerstatter durch Telefonanrufe der Verwarnten.

In dem auf die Ahndung geringfügiger Ordnungswidrigkeiten gerichteten Verwarnungsverfahren ist die Angabe der Beweismittel (Zeugen u. a.) weder vorgeschrieben noch untersagt. Für die Nennung der Zeugen spricht zwar im Grundsatz das Rechtsstaatsprinzip, das es angezeigt erscheinen läßt, einem mit einer Sanktion (Verwarnungsgeld) belegten Bürger auch die Grundlagen der gegen ihn gerichteten Anzeige zu nennen. Je nach Lage des Einzelfalls kann aber der Zeugenschutz vor dem Interesse eines Betroffenen, den Namen eines Zeugen zu kennen, überwiegen. Auf Antrag sollte daher nach Überprüfung der konkreten Sachlage von der Zeugenbenennung bei Verwarnungsgeldangeboten durch die Bußgeldstelle Abstand genommen werden.

Das Ministerium des Innern und für Sport hat sich der Auffassung des LfD angeschlossen. Die zuständige Stadtverwaltung will bei Verwarnungsgeldangeboten in Zukunft generell die Zeugen nicht mehr namentlich nennen und sie stattdessen nur noch als vorhanden oder „bekannt" vermerken.

Darüber hinaus sollte geprüft werden, ob auch in Bußgeldbescheiden, für die nach § 66 Abs. 1 Ziff. 4 Ordnungswidrigkeitengesetz die Bezeichnung der Beweismittel vorgeschrieben ist, auf das Hinzufügen der Wohnanschrift verzichtet werden kann. Bei der Bewertung des Beweismittels durch den Betroffenen wird es regelmäßig auf die Kenntnis der Wohnanschrift nicht ankommen. Gegenüber dem von der Rechtsordnung gebotenen Zeugenschutz und dem in der Verfassung begründeten Recht auf informationelle Selbstbestimmung lassen sich unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit für die Nennung der Wohnanschrift keine gewichtigen Gründe oder ein überwiegendes Interesse der Allgemeinheit finden. Zu vergleichbaren Fragen im Strafbefehlsverfahren s. unten Tz. 7.3.6.

5.4 Datei gewalttätiger Fußballanhänger „Hooligans"

Die Gewalt in Fußballstadien hat sich in den vergangenen Jahren ausgebreitet und nimmt teilweise erschreckende Formen an. Auch außerhalb der Fußballstadien führt das Auftreten gewaltbereiter – meist jugendlicher – Fußballanhänger in den Städten, die Austragungsorte sind, zu unerträglichen Zuständen. Die von dem Rowdytum betroffenen Bürger in den Fußballstadien und in den Straßen der Innenstädte haben – wie alle Menschen – ein Recht auf Sicherheit, dem eine entsprechende Verpflichtung des Staates gegenübersteht, durch geeignete Maßnahmen, den erforderlichen Schutz zu gewähren.

Die in diesem Zusammenhang begangenen Straftaten reichen üblicherweise von Landfriedensbruch, Hausfriedensbruch und Sachbeschädigung bis zu räuberischem Diebstahl sowie schwerer und gefährlicher Körperverletzung.

Zur Durchführung eines Ermittlungsverfahrens gegen eine Vielzahl gewalttätiger Fußballanhänger wegen der genannten Straftaten hat das Polizeipräsidium Kaiserslautern bereits im Dezember vergangenen Jahres durch eine Sofortenrichtungsanordung eine nichtautomatisierte Datei als Lichtbilddatei eingerichtet und bei der DSK angemeldet. Nach Prüfung von Zweck und Inhalt der Datei bestanden aus der Sicht des Datenschutzes keine Bedenken. In der Zwischenzeit wurde eine endgültige Errichtungsanordnung erlassen, in der der Zweck der Datei auf das Erkennen und Identifizieren von Störergruppen und Störern ausgedehnt wurde, um rechtzeitig polizeiliche Maßnahmen zur Abwehr im Einzelfall bestehender Gefahren treffen zu können. Rechtsgrundlagen sind die einschlägigen Eingriffsermächtigungen in der Strafprozeßordnung und im Polizeiverwaltungsgesetz. Auch der LfD erhebt insoweit keine Einwendungen.

Nunmehr hat sich allerdings gezeigt, daß der Gefährdungslage mit einzelnen und manuellen Dateien der Polizeibehörden in den Austragungsorten nicht mehr wirksam begegnet werden kann, weil Täter und Tätergruppen bundes- und auch europaweit auftreten. Auf Beschluß der „Ständigen Konferenz der Innenminister und Senatoren der Länder" (IMK) vom 15. Dezember 1990 wurde u. a. der Arbeitskreis II beauftragt zu prüfen, ob und in welcher Form von den Polizeien des Bundes und der Länder Informationen über Personen, die wegen Gewalttätigkeiten im Zusammenhang mit sportlichen Ereignissen in Erscheinung getreten sind, zur Gefahrenabwehr und zur Verfolgung von Straftaten vorgehalten und übermittelt werden können. Dabei wurde ausdrücklich bestimmt, daß die Datenschutzbeauftragten des Bundes und der Länder an der Prüfung beteiligt werden sollten. Dies ist im weiteren Fortgang jedoch nur in sehr unvollkommener Weise geschehen. Ergebnis der weiteren Beratungen eines eingesetzten Unterausschusses, der seinerseits einen Ad-hoc-Ausschuß „Recht der Polizei" gebildet hat, ist im wesentlichen die Absicht, eine Datei „Gewalttäter Sport" als Verbunddatei beim BKA einzurichten. In dem schriftlichen Bericht des Ad-hoc-Ausschusses heißt es „Aus zeitlichen Gründen konnten die Datenschutzbeauftragten des Bundes und der Länder nicht beteiligt werden". Dieses Verfahren muß umso mehr verwundern, als die Datenschutzbeauftragten bislang keinerlei Anlaß zu der Vermutung gegeben haben, daß ihre Beteiligung zu nennenswerten Verzögerungen führt. Die bisherige Ausschaltung der Daten-

schutzbeauftragten ist aber auch von der Sache her zu bedauern, weil die Beratung in datenschutzrechtlicher Hinsicht – übrigens die Wahrnehmung einer gesetzlichen Aufgabe – bekanntermaßen umso effektiver ist, je früher sie erfolgt. Gibt es kontroverse Punkte, so lassen sich diese erfahrungsgemäß bei frühzeitiger Erörterung leichter abklären und evtl. bereinigen, als wenn sich die gegenseitigen Standpunkte erst verfestigt haben oder wenn sich durch ein Fortschreiten der Planung Änderungen, die aus datenschutzrechtlicher Sicht geboten sind, nur noch mit erheblichem Zusatzaufwand verwirklichen lassen.

Der LfD bittet deshalb die Landesregierung, bei der Entwicklung künftiger Konzeptionen auf der Länderebene – soweit sie für den Datenschutz von Bedeutung sind – dafür einzutreten, daß die Beteiligung der Datenschutzbeauftragten zu einem möglichst frühen Zeitpunkt erfolgt.

Nach den bisherigen Erörterungen im Arbeitskreis II sollen die Polizeien der Länder die Daten in eigener Verantwortung zur Speicherung in einer im BKA geführten Verbunddatei anliefern. Gleiches gilt für den Abruf von Daten, so daß sich die Zulässigkeit insoweit nach Landesrecht – hier nach dem PVG – richtet.

Im wesentlichen sollen Daten aus einschlägigen Ermittlungsverfahren, Verurteilungen und Bußgeldbescheiden, Stadionverboten, Ingewahrsamnahmen sowie aus der Sicherstellung bzw. Beschlagnahme von Waffen gespeichert werden. Neben den Personalien der Betroffenen werden näher festgelegte sachliche Hinweise gespeichert.

Im Rahmen der nunmehr erbetenen Stellungnahme vertrat der LfD die Auffassung, daß die Verbunddatei unter Berücksichtigung der rheinland-pfälzischen Rechtslage zulässig ist. Diese Beurteilung konnte allerdings nur auf der Basis der seiner Behörde zur Verfügung stehenden Unterlagen erfolgen, zu denen noch nicht der Text der beabsichtigten Errichtungsanordnung gehört.

Die Abwägung der Sicherheitsrechte der Bürger mit den Belangen der von der beabsichtigten Datenverarbeitung Betroffenen gestattet keine grundsätzlichen Zweifel, zumal die verhältnismäßig geringe Sensitivität die Schwere des Eingriffs höchstens auf einer mittleren Ebene hält.

Auch an der teilweise angezweifelten Geeignetheit der Datei als Maßnahme zur Abwehr der in Frage stehenden Gefahren und zur vorbeugenden Bekämpfung von Straftaten ist nach Auffassung des LfD nach den ihm zur Verfügung stehenden Informationen nicht zu zweifeln. Durch die Feststellung der Personalien an Kontrollstellen, bei Zwischenfällen außerhalb der Stadien vor Spielbeginn sowie anhand vorhandenen Bildmaterials oder von Hinweisen begleitender Beamter aus den Herkunftsstädten können Abfragen erfolgen, die zunächst einmal Erkenntnisse für organisatorische und taktische Maßnahmen (z. B. Personalverstärkungen an bestimmten besonders gefährdeten Stellen) liefern. In Einzelfällen wird die Prüfung erleichtert, ob bestimmte Personen nach Waffen durchsucht, vorübergehend in Gewahrsam genommen, des Platzes verwiesen oder lediglich weiter beobachtet werden sollen. Gerade für präventive Maßnahmen ist es von erheblicher Bedeutung zu wissen, ob es sich z. B. um sog. Rädelsführer handelt oder wie sich bestimmte Personen gegenüber polizeilichen Maßnahmen verhalten. Schließlich sind die Erkenntnisse auch für Maßnahmen zur Eigensicherung der eingesetzten Beamten geeignet und erforderlich.

In der Errichtungsanordnung sollte festgelegt werden, daß personenbezogene Daten nur über sog. „reisende Täter", also über solche Personen eingestellt werden, von denen mit hinreichender Sicherheit angenommen werden kann, daß sie nicht nur in einem Stadion auftreten. Auch sollte bei jedem Datensatz auf dem Protokollband die eingebende Dienststelle und der Beamte festgehalten werden, wobei dieser Datensatz von anderen Dienststellen wiederum nur protokolliert verändert werden darf. Erkenntnisse, die zu einer Löschung führen, sollten die speichernde Stelle auch dann zur Löschung berechtigen, wenn andere Stellen Daten hinzugespeichert haben. Es muß auch sichergestellt werden, daß Rückmeldungen der Justiz an die Polizei für die Prüfung einer evtl. Löschung der Datensätze berücksichtigt werden können. Für die Prüfung, ob eine Löschung im Einzelfall geboten ist, sollten mit den Datensätzen Wiedervorlagefristen gespeichert werden. Ferner sollten Fußballvereine auf den Inhalt der Verbunddatei nicht automatisiert zugreifen dürfen. Schließlich sollte eine angemessene zeitliche Befristung vorgesehen werden, die es ermöglicht, zwischenzeitliche Erfahrungen bei einer evtl. Fortführung der Datei durch Änderungen zu berücksichtigen.

5.5 Weitergabe von personenbezogenen Daten aus Telefonüberwachungen

Strafermittlungsverfahren gegen größere Täterkreise wie bei Banden- und Rauschgiftkriminalität, weitverzweigten Betrugsverfahren u. a. erfordern in einer zunehmenden Zahl von Fällen die richterliche Anordnung der Telefonüberwachung unter den Voraussetzungen des § 100 a StPO. Diese Voraussetzungen hat der Gesetzgeber eng gezogen: Es müssen bestimmte Tatsachen den Verdacht einer Straftat begründen, die wegen ihrer besonderen Bedeutung in einem abschließenden Katalog im Gesetz aufgeführt ist (sog. Katalogtaten). Als für die Staatsanwaltschaft ermittelnde Stelle richtet die Polizei in jedem Falle eine Datei – zumeist unter Verwendung eines PC – ein und erstellt eine Errichtungsanordnung, die sie in verkürzter Form gemäß § 10 Abs. 2 LDatG beim LfD anmeldet. Angesichts des mit der Telefonüberwachung verbundenen besonders schweren Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen ist bei der Prüfung der datenschutzrechtlichen Zulässigkeit der jeweils beabsichtigten Anwendungen ein strenger Maßstab anzulegen. Dies gilt auch für die Datensicherung, für die Abrufberechtigung und die strenge Zweckbindung der Daten.

Es ist zu begrüßen, daß die datenschutzrechte Verarbeitung der aus Maßnahmen der Telefonüberwachung gewonnenen Daten in einer generellen Rahmenerrichtungsanordnung zur Vereinfachung und Vereinheitlichung der nach wie vor erforderlichen Einzelanmeldungen geregelt wird und daß der Behörde des LfD Gelegenheit zur Stellungnahme gegeben wurde. Es ist vorgesehen, daß eine Vermischung der Daten aus der Telefonüberwachung mit Daten aus anderen Dateien, die zur Durchführung des Ermittlungsverfahrens errichtet worden sind, ausgeschlossen ist. Damit ist im Grundsatz dem Umstand Rechnung getragen, daß diese Daten mit außergewöhnlichen Mitteln und unter erschwerten gesetzlichen Voraussetzungen erhoben wurden. Auch die Möglichkeit der Konvertierung der Daten auf andere Programme ist ausgeschlossen.

Erhebliches Gewicht aus der Sicht des Datenschutzes kommt der Frage der Verwendung der Daten zu Zwecken außerhalb des jeweiligen Strafermittlungsverfahrens zu. Während die Verwendung sog. „Zufallsfunde" zur Strafverfolgung auch gegen dritte Personen durch die Rechtsprechung zugelassen wird, wenn es sich um die Verfolgung von Katalogtaten handelt, und ansonsten immerhin die mittelbare Verwertung als Grundlage weiterer Ermittlungen möglich ist, gibt es für eine Verwendung zu präventivpolizeilichen Zwecken weder im Strafverfahrensrecht noch im materiellen Polizeirecht eine ausdrückliche Regelung. Konkret geht es darum, ob die bei einer Telefonabhörmaßnahme erlangte Kenntnis von einer bevorstehenden erheblichen und konkreten polizeilichen Gefahr verwendet werden darf oder nicht. Hier entsteht ein Konflikt zwischen dem Recht des betroffenen Verdächtigen auf informationelle Selbstbestimmung, das durch diese Nutzung der Daten beeinträchtigt werden kann, und dem Recht auf Sicherheit, das – ebenfalls aus der Verfassung hergeleitet – demjenigen gegenüber dem Staat zusteht, dessen Rechtsgüter durch rechtswidrige Handlungen bedroht sind. Danach muß das Verhindern von Straftaten als Aufgabe der Polizei als nicht minder wichtige Aufgabe anzusehen sein, wie die Verfolgung von Straftaten. Im Grundsatz ist auch bei einer Nutzung der aus Telefonabhörmaßnahmen gewonnenen Daten der Grundsatz der Verhältnismäßigkeit zu berücksichtigen, so daß es nicht zulässig sein kann, sie zur Verhinderung von Bagatellstraftaten mit unerheblicher Schadensgefahr zu verwenden. Unter Berücksichtigung dieser Überlegungen ist die Verwendung der Daten zur konkreten Gefahrenabwehr für zulässig zu halten, nicht hingegen für Maßnahmen der vorbeugenden Straftatenbekämpfung.

Dabei kann davon ausgegangen werden, daß es für die Abwehr einer konkreten Gefahr in der Regel nicht notwendig ist, die aus der Abhörmaßnahme gewonnenen Daten hierfür gesondert zu speichern. Zumindest sind sie nach Beseitigung der Gefahr zu löschen, soweit sie nicht zwischenzeitlich aus anderer Quelle erhoben werden konnten.

Um bis zu einer endgültigen gesetzlichen Regelung dieses Fragenkomplexes aus rechtsstaatlichen Gründen ein höheres Maß an Transparenz zu schaffen, hat der LfD sowohl dem Minister des Innern und für Sport wie dem Justizminister vorgeschlagen, einstweilen durch eine zu veröffentlichende Verwaltungsvorschrift vorzusehen, daß die Verwendung von personenbezogenen Daten aus Telefonabhörmaßnahmen zu anderen als Strafverfolgungszwecken nur vom Staatsanwalt unter den dargestellten Voraussetzungen zugelassen werden darf. Nur dann, wenn Gefahr im Verzuge ist und die zuständige Staatsanwaltschaft nicht erreicht werden kann, soll die speichernde Polizeibehörde selbst entscheiden dürfen. Es muß sich aber dann um die Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit handeln.

5.6 Staatliche Untersuchungsstelle für Blutalkohol

Werden aufgrund der §§ 81 a und 81 c der Strafprozeßordnung oder des § 46 OWiG Blutproben entnommen, so sind diese gemäß einer gemeinsamen Verwaltungsvorschrift des Ministeriums der Justiz und des Ministeriums des Innern vom 17. Oktober 1990 (JM 4103 – 4 – 57/90 – MinBl. S. 391), bei deren Vorbereitung die DSK nicht beteiligt worden war, der Staatlichen Untersuchungsstelle für Blutalkohol bei dem Institut für Gerichtliche Medizin der Johannes Gutenberg-Universität Mainz zur Durchführung der Blutuntersuchung zuzuleiten (Nummer 14 der VV). Aufgrund dieser Verwaltungsvorschrift werden bei der Untersuchungsstelle Protokollbücher über die Kennzeichnung der Proben und die Ergebnisse der Alkoholbestimmung geführt. Diese sind nach Nummer 15 der VV zehn Jahre lang aufzubewahren. Daneben existieren die Aktenunterlagen und eine PC-Datei, die der Dokumentation und der Unterstützung des Verfahrens bei der Untersuchungsstelle dient und von dieser im Juli 1990 bei der DSK angemeldet wurde. Als Rechtsgrundlage für diese Datei sind nicht die genannten Bestimmungen der Strafprozeßordnung heranzuziehen und ebensowenig die zitierte Verwaltungsvorschrift; sie ist daher nach den Bestimmungen des LDatG zu beurteilen. Die DSK hat unmittelbar nach Kenntnisnahme der Anmeldung Bedenken gegen das Fehlen einer Löschungsregelung geltend gemacht und im Hinblick auf die besondere Sensibilität der Daten Zweifel angemeldet, ob es erforderlich ist, ungeachtet der Löschungsregelung in § 13 Abs. 4 LDatG in allen Fällen eine „Aufbewahrungsfrist" von zehn Jahren vorzusehen. Eine kürzere Zeit sollte insbesondere in den Fällen gelten, in denen keine strafrechtlich oder verkehrsrechtlich relevanten Untersuchungsergebnisse festgestellt wurden. Weiterhin wurde u. a. die Frage nach der Protokollierung von Eingaben und Abfragen aus der Datei gestellt sowie nach den technischen und organisatorischen Vorkehrungen durch die die Einhaltung von Löschungsfristen gewährleistet wird. Das Ministerium des Innern und für Sport und die Staatliche Untersuchungsstelle haben der DSK zugestimmt, daß, dem Zweck der Datei entsprechend, nicht alle für die Erstellung des jeweiligen Gutachtens erforderlichen Daten nach der Fertigung des Abschlußberichts weiter gespeichert bleiben müssen und daß auch im Hinblick auf die Art des Delikts eine unterschiedliche Speicherungsdauer angezeigt ist. Hierzu wurde nunmehr ein Vorschlag für differenzierte Speicherungszeiten von einem Monat sowie von drei und von zehn Jahren vorgelegt, der zumindest im Grundsatz aus der Sicht des Datenschutzes zu begrüßen ist.

Weitere Festlegungen in der Anmeldung bleiben erörterungsbedürftig.

In dem Formblatt für den Antrag der ermittelnden Polizeidienststellen an die Staatliche Untersuchungsstelle sind Angaben über „von dem jetzigen Vorfall unabhängige Krankheiten oder Leiden" vorgesehen. Diesen entspricht in dem angemeldeten Datensatz das Merkmal „Ärztliche Beurteilung des Probanden" (Nummer 25). Erforderlich dürften nach Auffassung des LfD jedoch nur solche Feststellungen sein, die in einem erkennbaren Zusammenhang mit der Untersuchung stehen. Da es sich um medizinische Daten handelt, ist bei der Erforderlichkeitsprüfung insoweit ein besonders strenger Maßstab anzulegen. Auch bedarf es der Klärung, weshalb in dem an die Staatliche Untersuchungsstelle zu versendenden Formblatt der Beruf des Probanden anzugeben ist.

5.7 Speicherung und Übermittlung von Daten bei Selbstmordversuchen

Schon 1988 erfolgte nach intensiver Diskussion der damit zusammenhängenden datenschutzrechtlichen Fragen, die auch in der Öffentlichkeit geführt wurde, die Neudefinition des personengebundenen Hinweises „Freitodgefahr" (PHW) im polizeilichen Informationssystem. Vorangegangen war ein Beschluß des Arbeitskreises II der Innenministerkonferenz. Daraufhin hatte auch das Landeskriminalamt eine umfassende Überprüfung der entsprechenden Datensätze vorgenommen, was zu einer Reduzierung auf etwa 375 Speicherungen geführt hat. Die anschließend von der DSK durchgeführte stichprobenartige Überprüfung dieser noch verbliebenen Speicherungen bei einem Polizeipräsidium führte zu keiner Beanstandung der Speicherungspraxis. Alle Polizeidienststellen des Landes waren bereits vor dem Beschluß des Arbeitskreises II angewiesen, eine Löschung vorzunehmen, soweit kein weiterer Suizidversuch des Betroffenen in dieser Zeitspanne der Polizei bekannt wurde. Zwischenzeitlich wurde auf Vorschlag des Landeskriminalamtes die Frist in den Fällen verlängert, in denen der Betroffene im Zusammenhang mit einem Rauschgiftdelikt bekannt wurde. Angesichts der Entwicklung der Rauschgiftkriminalität und der damit verbundenen dramatisch steigenden Zahl von Rauschgifttoten ist die Praxis als Maßnahme der vorbeugenden Gefahrenabwehr verständlich und zu begründen. Als Rechtsgrundlage kann allerdings nicht § 25 a Abs. 1 Nr. 2 PVG herangezogen werden, wonach personenbezogene Daten „zur vorbeugenden Bekämpfung von Straftaten" gespeichert werden können; Selbstmord ist grundsätzlich keine Straftat. Die Löschungsfrist soll sich in diesen Fällen nach der für die Gesamtakte festgelegten Speicherungsdauer richten.

Zu der Übermittlung personenbezogener Daten durch die Polizei an die Sozialpsychiatrischen Dienste der Gesundheitsämter ist bereits im 12. Tätigkeitsbericht Stellung genommen worden (vgl. Tz. 5.4.1). Damals war es das Ergebnis von Gesprächen der DSK mit Vertretern des Ministeriums des Innern und für Sport und des Ministeriums für Umwelt und Gesundheit, daß Daten von Personen, die einen Selbstmordversuch unternommen haben, von der Polizei grundsätzlich nur noch mit ihrer Einwilligung an die Sozialpsychiatrischen Dienste der Gesundheitsämter übermittelt werden. In einem Rundschreiben an die Bezirksregierungen und weitere Polizeibehörden weist das Ministerium des Innern und für Sport darauf hin, daß eine Übermittlung (ansonsten) nur in Frage kommt, wenn sich der Betroffene in einem die freie Willensbildung ausschließenden Zustand befindet und somit die Ingewahrsamnahme zulässig sowie angemessen wäre und wenn nach der Entlassung aufgrund der Umstände des Einzelfalles durch Sorgeberechtigte oder Ehepartner/Verwandte offenkundig kein genügender Rückhalt bestehen dürfte, der geeignet wäre, einem neuen Selbsttötungsversuch vorzubeugen.

Um jedoch eine Krisenintervention und eine – vom Betroffenen gewünschte – nachfolgende Betreuung zu ermöglichen, sollen Polizei und Gesundheitsämter eng zusammenarbeiten. Diesem Ziel soll ein zu erarbeitendes Informationsblatt dienen, mit dem die Betroffenen kurz und ohne Amtlichkeitscharakter über örtliche Hilfsmöglichkeiten durch staatliche und private Stellen – auch Selbsthilfegruppen – informiert werden.

5.8 Unzulässige Halterabfragen in ZEVIS

Ein Ehepaar wandte sich an den LfD, weil es nach vorübergehendem Parken seiner Kraftfahrzeuge in der Nähe eines Baggersees von dem nutzungsberechtigten Surf-Club ein Schreiben mit der Aufforderung erhielt, dies künftig zu unterlassen. Das Ehepaar konnte sich nicht erklären, wie der Club aufgrund der Fahrzeugkennzeichen in den Besitz der Halterdaten gekommen sein konnte.

Eine Nachfrage bei der zuständigen Kreisverwaltung ergab, daß dort keine Halterabfragen vorgenommen wurden und auch keine entsprechenden Mitteilungen an den Surf-Club erfolgten. Wie weiter festgestellt werden konnte, erfolgten die erforderlichen Halterabfragen bei dem Zentralen Verkehrs-Informationssystem (ZEVIS), das bei dem Kraftfahrtbundesamt in Flensburg geführt wird. Dort wird jede Halterabfrage protokolliert, so daß festgestellt werden konnte, daß die Abfrage von einer nahen Polizeidienststelle vorgenommen worden ist. Dort war jedoch der Versuch, weiter festzustellen, wer in welchem Zusammenhang die Abfrage veranlaßte, bislang erfolglos.

Die bei ZEVIS erfolgende Protokollierung aller Halterabfragen führt nur bis zu dem Terminal, von dem aus die jeweilige Abfrage erfolgt. Um darüber hinaus ein Minimum an Kontrolle zu gewährleisten, fragt ZEVIS vor jedem fünfzigsten Datenabruf nach näheren Angaben, insbesondere nach den Gründen des Abrufs. Gleichwohl bleibt ein Rest an Unsicherheit. Bei der Vielzahl der

Abfragen und angesichts der Arbeitsbelastung in den polizeilichen Einsatzzentralen, in denen sich die Abfrageterminals befinden, wird man nicht verlangen können, daß jede Abfrage dort zusätzlich so protokolliert wird, daß die veranlassende Stelle daraus ersichtlich ist. Zudem wäre auch eine solche Vorkehrung nicht lückenlos, da nicht alle mit einer Abfrage verbundenen Vorgänge aktenmäßig festgehalten werden.

Solange keine praktikable und die Polizei nicht zusätzlich belastende Kontrollmethode gefunden ist, bleibt nur die Empfehlung, die Polizeibehörden mögen ihre Beamten regelmäßig und in geeigneter Weise darauf hinweisen, daß Halterabfragen, die keine Grundlage in den einschlägigen polizei- und verkehrsrechtlichen Vorschriften finden, unzulässig sind.

Was die oben dargestellten Abfragen anbetrifft, so sind die Ermittlungen zur präzisen Sachverhaltsaufklärung noch im Gange. Nachdem bisher kein polizeilicher Vorgang festgestellt werden konnte, der die Abfragen hätte begründen können, ist nach dem jetzigen Stand die Möglichkeit offen, daß sie unzulässig waren, insbesondere weil nach wie vor nicht auszuschließen ist, daß ein Zusammenhang mit dem von den betroffenen Eheleuten beanstandeten Schreiben besteht.

Sollte es sich – wofür jedoch z. Z. keine konkreten Anhaltspunkte vorliegen – um den Schutz privater Rechte im Sinne des §§ 25 a Abs. 1 Ziff. 3 i. V. m. § 1 Abs. 2 PVG gehandelt haben, so wäre eine Halteranfrage in der vorgenommenen Form nicht zulässig gewesen, weil gerichtlicher Schutz auf jeden Fall rechtzeitig zu erlangen gewesen wäre und überdies ein wie auch immer geartetes privates Recht ohne polizeiliche Hilfe unschwer hätte verwirklicht werden können (§ 1 Abs. 2 PVG).

5.9 POLADIS

Das System POLADIS (Polizeiliches anwenderorientiertes dezentrales Informations-System) wurde bereits im 12. Tätigkeitsbericht unter Tz. 5.2.1 als ein bei der Kreisverwaltung der Donnersbergkreises und beim Polizeipräsidium Mainz eingeführtes Pilotprojekt vorgestellt. Es ersetzt die Registrierung und Dokumentation der polizeilichen Vorgänge in einer Vielzahl von unterschiedlichen Tagebüchern, Sammlungen und manuellen Dateien. Die dadurch erreichte bessere Übersicht beschleunigt und erleichtert nicht nur die polizeiliche Arbeit, sie kann bei Beachtung entsprechender Vorkehrungen auch zu einem verbesserten Datenschutz insbesondere durch mehr Transparenz der Vorgänge und durch eine wirksamere Kontrolle beitragen. Zwischenzeitlich wurde das System – immer noch in der Phase der Erprobung und Entwicklung – auf den Ebenen der Polizeipräsidien, Schutzpolizeiinspektionen und Kriminalkommissariate in weiteren Fällen eingeführt. Dabei wurde es von der DSK und vom LfD mit verschiedenen Vorschlägen zur Verbesserung des Datenschutzes begleitet.

Ein ausreichender Datenschutz fordert den Einsatz nicht vernetzter Rechner auf der Ebene der Dienststellen. Zur Zeit sind die Systeme nicht miteinander vernetzt, so daß dieser Forderung entsprochen wird. Allerdings bestehen Anschlüsse an das Polizeifernschreibnetz und an das Landesdatenfernübertragungsnetz, so daß Texte aus der Anlage als Polizeifernschreiben weitergegeben werden. Auch ist es möglich, auf das zentrale Fahndungssystem INPOL/POLIS zuzugreifen. Ein Zugriff von einer POLADIS-Anlage auf eine andere ist jedoch nicht möglich. Soweit für die Zukunft Überlegungen bestehen, die Systeme an ein Datennetz anzuschließen, welches das veraltete Polizeifernschreibnetz ersetzt, zwingen diese zu weiteren Überlegungen bezüglich des technischen und organisatorischen Datenschutzes. Auf keinen Fall dürfen hiermit Zugriffsmöglichkeiten von einem Rechner auf den anderen verbunden sein. Hierüber konnte schon jetzt mit dem Ministerium des Innern und für Sport Übereinstimmung erzielt werden.

Grundsätzlich soll aus der Sicht des Datenschutzes ein Zugriff auf die gespeicherten Daten innerhalb einer Dienststelle nur für die mit der Vorgangsbearbeitung befaßte Teileinheit möglich sein. Vorgangsverwaltungsdaten dürfen demnach nur für das jeweilige Vorhaben oder den konkreten Vorgang genutzt werden. Jedenfalls darf die eigenständige Verwendung von Vorgangsverwaltungsdaten zu anderen Zwecken nicht zu einer Umgehung der gesetzlichen Voraussetzungen für die jeweilige polizeiliche Tätigkeit führen. Dabei wird nicht verkannt, daß der damit angesprochene Grundsatz der funktionalen Trennung, der aus dem Zweckbindungsgrundsatz folgt, auch vor dem Hintergrund der ganzheitlichen polizeilichen Aufgabenerfüllung gesehen werden muß, der durch Doppelfunktionalität (Schutz- und Kriminalpolizei) bestimmt wird. Voraussetzung ist eine ausreichende Rechtsgrundlage für Zweckänderungen. Nachdem das Ministerium des Innern und für Sport ebenfalls überzeugt ist, daß über die einschlägigen Regelungen zur Datensicherheit hinaus weitere technische Vorkehrungen zu treffen sind, um die Zweckbindung bei der Datenverarbeitung sicherzustellen, wird eine Log-Datei eingesetzt, in der protokolliert wird, wer wann auf welchen Datensatz mit welcher Aktivität (Lesen, Ändern, Anfügen) zugegriffen hat. Auch hiermit wird einer aktuellen datenschutzrechtlichen Forderung entsprochen. Es wäre wünschenswert, wenn sich die Protokollierung zusätzlich auf den Abfragegrund erstrecken könnte.

Die Archivierung der gespeicherten Vorgangsdaten nach drei Monaten ist jetzt ebenso realisiert wie der Änderungsschutz für Originaldokumente und Vorgänge.

Offen ist nach wie vor die Nutzung der archivierten Daten. Diese Frage bedarf noch der abschließenden Erörterung mit dem Ministerium des Innern und für Sport.

Nach dem bisher bekannten Vorschlag des LKA soll bei der Archivierung die Datenbank „Vorgang" auf Bänder übertragen und dem aktuellen Zugriff zunächst vollständig entzogen werden. Gleichzeitig wird eine Datenbank „Archiv" angelegt, in der von den ursprünglichen im Bereich der Vorgangsverwaltung vorhandenen 251 Datenfeldern noch 144 Datenfelder (also 57 %) belegt sind, von denen allerdings nur 87 am Bildschirm angezeigt und damit auch derzeit nur abgerufen werden können. Die Datei „Archiv" ist aufgeteilt in einen Bereich „Archiv, Vorgangsverzeichnis", der grundsätzlich im Zugriff der gesamten Dienststelle steht, und in einen Bereich „Archiv, Statistik, Recherche", der nur vom Systemverwalter selbst ausgewertet werden kann. Im Bereich „Archiv, Vorgangsverzeichnis" sind dann noch die genannten 87 Datenfelder belegt; das entspricht etwa einem Drittel der ursprünglich vorhandenen Datenfelder. Im Bereich „Archiv, Statistik, Recherche" sollen es noch 117 Datenfelder, prozentual also etwa 50 % sein. Eine Löschung dieser Datenbestände im Bereich „Archiv" soll nach fünf Jahren erfolgen.

Trotz mengenmäßiger Reduktion im Bereich von etwa zehn Datenfeldern zeigen diese Quantitäten, daß die archivierten Daten keinesfalls nur als Aktennachweis- oder Aktenauffindungssystem fungieren. Dies gilt auch für die inhaltliche Betrachtung der Daten. Es handelt sich um detaillierte Angaben zur Person der Betroffenen (Anzeigenerstatter, Zeugen, Geschädigte, Tatverdächtige etc.), einschließlich genauer Wohnanschrift, Vor-, Familien- und Geburtsnamen, Stellung im Vorgang, sowie um Angaben zu diesem selbst, die ihn detailliert bezeichnen, mit Teilinformationen über den Verkehrsunfall, einschließlich Fahrzeugart, Kennzeichen und Sicherstellung. Eine erneute, aus Gründen des Datenschutzes im ISM veranlaßte Überprüfung hat jetzt die Entbehrlichkeit der Abrufmöglichkeit von archivierten Informationen über Alkoholeinwirkung, Sicherheitsleistung, körperliche Unfallfolgen und Schadenshöhe ergeben.

Nach wie vor sind damit Vorgangsdaten, die fünf Jahre im jederzeitigen Zugriff der gesamten Polizeidienststelle – und nicht mehr nur der den Vorgang ursprünglich bearbeitenden Teilstelle – verbleiben sollen, als eigenständiges Informationssystem anzusehen, das einer ebenso eigenständigen Beurteilung hinsichtlich der Erforderlichkeit sowie der etwa nötigen Zweck- und Zugriffsbeschränkung zu unterziehen ist.

Dieses Problemfeld wurde in allen seinen datenschutzrechtlichen Konsequenzen bei einer örtlichen Besichtigung durch den LfD im Juni 1991 ganz deutlich. Das Ministerium des Innern und für Sport hat nunmehr – nachdem die Überlegungen des LfD hierzu auch schriftlich formuliert wurden – zu den einzelnen Daten eine detaillierte Zweckbestimmung erarbeitet. Jetzt wird anhand der Merkmale des § 25 a PVG zu prüfen sein, ob die gesetzlichen Voraussetzungen hinsichtlich aller gespeicherter Daten erfüllt sind. Dabei muß auch überlegt werden, ob innerhalb des Bereichs „Archiv, Vorgangsverzeichnis" im allgemeinen Zugriff der gesamten Polizeidienststelle nur Informationen belassen werden, die für das Auffinden von Vorgängen erforderlich sind. Es sollte auch auf alle Fälle eine Zugriffsbeschränkung für besonders sensible Daten, wie z.B Verkehrsunfallflucht, u. a., eingeführt werden, die den Zugriff auf abgeschlossene Vorgänge nur bestimmten Geschäftsbereichen und Personengruppen vorbehält. Nutzungen, die über den Zweck des Aktenauffindens hinausgehen, sollten im Archivbereich nur zugelassen werden, wenn sie zu genau bezeichneten, mit § 25 a Abs.1 Nr. 1 bis 5 PVG übereinstimmenden Zwecken und unter den dort festgelegten Voraussetzungen erfolgen. Das muß auch für den Direktzugriff auf Finder, Anzeiger, Zeugen und Auskunftspersonen gelten. Die Verhandlungen mit dem Ministerium des Innern und für Sport sind zwischenzeitlich fortgeschritten. Das Ministerium des Innern und für Sport prüft die Möglichkeiten einer engen Zugriffsbeschränkung, die darin bestehen könnte, Abfragen aus dem Bereich „Archiv, Vorgangsverzeichnis" nur durch das Geschäftszimmer als zentraler Stelle in der Behörde zuzulassen.

Hinsichtlich der zeitlichen Dauer muß schließlich sichergestellt sein, daß nach Abschluß der Vorgangsbearbeitung Daten zur Dokumentation nur zu deren Zwecken, für Disziplinarverfahren und Schadenersatzansprüche unter Berücksichtigung der dafür geltenden Verfolgungs- und Verjährungsfristen verarbeitet werden. Insgesamt ist die Speicherungsdauer so kurz wie möglich zu halten.

5.10 Einsatzleit-, Informations- und Auskunftssystem (ELIAS)

Im Jahre 1983 wurde ELIAS in Rheinland-Pfalz erstmals bei dem Polizeipräsidium Mainz im Rahmen eines Konzepts computerunterstützter Einsatzleitzentralen eingeführt, um Einsatzplanung und Einsatzlenkung zu vereinfachen und zu verbessern (vgl. 9. Tb., Tz. 3.9). Das System speichert Einsatzprotokolle mit allen relevanten Informationen im Zusammenhang mit einem Ereignis, einschließlich personenbezogener Daten (Mitteiler von Ereignissen, Geschädigte, Zeugen oder Täter, die im Rahmen der Einsätze in Erscheinung treten, Einsatzprotokolldatei). Ferner werden örtliche Informationssysteme (PIP = Polizei-Informations-Pool) geschaffen, die Anschriften von Personen enthalten, die zu Bewältigung bestimmter polizeilicher Lagen als Ansprechpartner bzw. als Kräfte kurzfristig benötigt werden (z. B. spezielle Handwerker, Fachärzte, Dolmetscher). Die DSK hatte gegen das Vorhaben im Jahre 1983 nach Besichtigung und Erläuterung keine Bedenken erhoben.

In der Zwischenzeit hat sich ELIAS nach der Beurteilung der Anwender bewährt. Es wurde zusätzlich bei den Polizeipräsidien Ludwigshafen und Trier eingeführt. Im Juli vergangenen Jahres wurde die Errichtungsanordnung für die einzelnen Dateien des Polizei-Informations-Pools aktualisiert und von der DSK überprüft. Die einzeln dargestellten Dateien betreffen im wesentlichen Abschleppvorgänge, die Alarmkartei, einen Bezirksstrukturkalender u. a. mit Angaben über Behörden und öffentliche Einrichtungen, Hilfsorganisationen und Notdienste, Versorgungsbetriebe, lebenswichtige Betriebe, Verkehrseinrichtungen, ausländische Vertretungen, Dolmetscher, Gaststättenverzeichnis, Spezialistendatei, Wachbuch des Polizeiführers vom Dienst.

Die DSK hat es begrüßt, daß durch die nunmehr vorgenommenen Spezifizierungen eine Strukturierung der verschiedenen PIP-Dateien erfolgte, und keine grundsätzlichen Bedenken gegen die Anwendungen erhoben. Es wurde jedoch festgestellt, daß § 25 a PVG nicht in allen Fällen als geeignete Rechtsgrundlage anzusehen ist. Mit dem Ministerium des Innern und für Sport besteht Übereinstimmung, daß in das PVG bei der nächsten Novellierung in Anlehnung an eine entsprechende Regelung in Nordrhein-Westfalen (§ 11 GFDPol NW) eine Bestimmung zur „Erhebung von personenbezogenen Daten zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen" eingefügt werden soll. Nach den Feststellungen erfolgen im System ELIAS keine Protokollierungen wie etwa bei POLIS oder POLADIS. Bei Zugriffen auf die Datei PIP registriert der Rechner lediglich die Uhrzeit des Zugriffs sowie das Terminal, über das die Datei genutzt wurde. Damit ist aber eine datenschutzrechtliche Kontrolle sichergestellt; denn anhand der sog. Wachbücher kann der Beamte, der zur fraglichen Zeit Zugriff haben konnte, jederzeit identifiziert werden. Wie weiter festgestellt werden konnte, liegt die Zustimmung des zuständigen Personalrates vor, soweit in ELIAS personenbezogene Daten von Bediensteten gespeichert werden.

5.11 Organisatorische Maßnahmen

Wesentliche Zuständigkeiten im Bereich der Datenverarbeitung und des technischen und organisatorischen Datenschutzes wurden durch eine seit dem 1. Januar 1991 geltende Organisationsänderung bei den Polizeipräsidien in Rheinland-Pfalz zusammengefaßt. Die Aufgaben des neu eingerichteten Kommissariates 26 (K/26) sind vor allem :

- die Bearbeitung von Grundsatzfragen des Datenschutzes bei der Verbrechensbekämpfung,
- die Datenerfassung und Datenpflege bei zentralen Auskunftssystemen,
- die Verfahrenskontrolle für automatisierte Informationssysteme sowie
- die Führung der kriminalpolizeilichen personenbezogenen Sammlungen.

Durch die Bündelung der genannten Zuständigkeiten soll die Beachtung und Umsetzung einschlägiger Vorschriften durchgängig gewährleistet werden. Seitens des LfD wird damit die Erwartung schnellerer und damit wirksamerer Datenschutzkontrollen verbunden.

6 Verfassungsschutz

6.1 Überprüfung der automatisierten Datenverarbeitung beim Verfassungsschutz und Regelung der Protokollierung

Die Überprüfung der Personenarbeitsdatei (PAD) bei der Verfassungsschutzbehörde des Landes ergab, daß mit dem zum Zeitpunkt der Überprüfung installierten System und den eingesetzten Programmen keine maschinelle Protokollierung (Logging) möglich war sowie kein ausreichendes Zugriffsberechtigungsverfahren eingerichtet und somit die Anforderungen nach § 9 Abs. 1 Ziff. 3 LDatG (Speicherkontrolle) und Ziff. 7 (Eingabekontrolle) nicht erfüllt wurden. Vor dem Hintergrund der Umstellung des Verfahrens und der Anschaffung eines neuen Systems wurden von der DSK die aus datenschutzrechtlicher Sicht wichtigsten Defizite mitgeteilt, die im Interesse einer verbesserten Datensicherheit bei der Anschaffung eines neuen Systems zu beachten sind. Die Anforderungen der DSK wurden in die Ausschreibung für das neue System aufgenommen. Die Erfüllung der Anforderungen für eine jederzeitige Kontrolle von Veränderungen im Datenbestand wurde vom Hersteller der neuen Hard-und Software bestätigt, so daß für die Personenarbeitsdatei protokolliert wird, welche Benutzer, zu welchem Zeitpunkt Änderungen, Neuanlagen und Löschungen im System durchgeführt haben. Der Empfehlung der DSK wurde entsprochen, für die Protokolldatei eine Aufbewahrungsfrist von zwei Jahren festzulegen.

Die von der Personenarbeitsdatei und der Registratur getrennte Textverarbeitung sieht auch eine programmäßige Trennung der den einzelnen Schreibkräften zur Verfügung stehenden Bildschirmgeräte vor. Eine Nutzung ist nur durch eine dem Benutzer zugeordnete Benutzerberechtigung und ein persönliches Paßwort möglich.

Die PAD und die Registratur sind ihrerseits vom Auskunftssystem NADIS vollkommen getrennt. Löschungsüberprüfungen in NADIS und in der PAD erfolgen regelmäßig jeweils vierteljährlich. Bei jeder Änderung ist der jeweils geänderte Teil des Datensatzes ebenfalls gelöscht und nicht rekonstruierbar. Soweit Löschungen in der Datei der Registratur vorgenommen werden, verbleiben hinsichtlich der gelöschten Dokumente nur noch das Aktenzeichen, die Namen des Einsenders oder des Empfängers sowie der Vernichtungsvermerk mit Datum. Damit kann allenfalls die Tatsache der Korrespondenz mit einer bestimmten Person oder Einrichtung festgestellt werden, nicht jedoch der Korrespondenzinhalt. Die gefundene Lösung stellt sicher, daß eine – auch datenschutzrechtliche – Kontrolle der Löschung jederzeit erfolgen kann, ohne daß hierfür Inhalte mit zum Teil hochsensitiven Daten weiter gespeichert bleiben müssen.

6.2 Verbesserte Kontrollierbarkeit der NADIS-Bestände

NADIS ist eine Verbunddatei, die beim Bundesamt für Verfassungsschutz in Köln geführt wird. Nach § 6 Sätzen 4 und 5 des Bundesverfassungsschutzgesetzes trägt jede Verfassungsschutzbehörde die Verantwortung im Sinne des allgemeinen Datenschutzrechtes für die von ihr eingegebenen Daten. Dabei muß die eingebende Stelle feststellbar sein. Die Feststellbarkeit war schon zuvor hinsichtlich der jeweiligen Zuspeicherungen durch andere Verfassungsschutzämter insoweit gegeben, als diese sich aus den gespeicherten Aktenzeichen ergaben. Dies galt nicht für den jeweiligen Datensatz, der neben dem Namen, Wohnort und Geburtsdatum immerhin zusätzlich Angaben z. B. über das Bankkonto und das Kraftfahrzeug enthielt. Da diese Bestandteile des Datensatzes auch von anderen Ämtern verändert werden könnten, mußte auch hier die Trennung der Verantwortlichkeit zwischen dem Bundesamt und den verschiedenen Landesverfassungsschutzbehörden sichtbar gemacht werden. Die Einhaltung dieses Gebotes wurde überprüft.

7 Justiz

7.1 Allgemeines

Im Justizbereich werden in den verschiedensten Zusammenhängen besonders sensible Daten von Bürgern erhoben und gespeichert: Die Justizregister beispielsweise, vom Schuldnerverzeichnis bis zum Namensregister der Staatsanwaltschaften, vom Grundbuch bis zum Genossenschaftsregister, enthalten Daten, die für den sozialen Status der Betroffenen häufig sehr bedeutsam sind.

Es werden hier nicht nur Informationen gesammelt, es entstehen durch eigenes Handeln auch Informationen, die für andere staatliche Bereiche, insbesondere die Verwaltung, von Bedeutung sein können.

7.1.1 Erforderliche Rechtsgrundlagen fehlen

Bedauerlich ist, daß trotz der auch hier bestehenden Tendenz zur zunehmenden Automatisierung und den damit einhergehenden Gefährdungen des Persönlichkeitsrechts der Betroffenen sowie trotz häufiger Anmahnungen der Datenschutzbeauftragten nach wie vor viele erforderliche Rechtsgrundlagen fehlen bzw. vorhandene Rechtsgrundlagen nicht ausreichend präzisiert und dem Verhältnismäßigkeitsgrundsatz entsprechend in ihrer Wirkung beschränkt worden sind.

Die wichtigsten Defizite sollen einleitend nur kurz angesprochen werden:

Die Strafprozeßordnung enthält nach wie vor nur unzureichende Regelungen der Datenverarbeitung durch Gerichte und Staatsanwaltschaften; ein Justizmitteilungsgesetz, das die Übermittlungen sowohl aus dem Bereich der Ziviljustiz wie dem der Strafjustiz an andere Stellen regeln soll, steht nach wie vor aus. Das Gesetz über das Schuldnerverzeichnis, mit dem § 915 ZPO ergänzt werden soll und das dringend erforderlich ist, wird nach wie vor in Ausschüssen des Deutschen Bundestages diskutiert. Eine Verabschiedung ist noch nicht abzusehen.

Ohne die genannten datenschutzrechtlich wichtigen Gesetze ist es kaum möglich, die verfassungsrechtlichen Anforderungen zum Schutz des informationellen Selbstbestimmungsrechts im Justizbereich in der Praxis zufriedenstellend zu realisieren.

7.1.2 Richterliche Unabhängigkeit bei der Nutzung von EDV

Im Bereich der Rechtsprechung nimmt die Tendenz zu, durch EDV-Einsatz (insbesondere durch PC) Arbeitsvorgänge zu erleichtern und zu beschleunigen.

Auch in diesem Zusammenhang stellen sich eine Reihe von Fragen, die das Persönlichkeitsrecht der Bürger betreffen:

Verstärkt der Einsatz der EDV die Tendenz zu „schematisierten" Fallbeurteilungen, die nicht mehr ausreichend am Einzelfall und an der Einzelfallgerechtigkeit orientiert sind? Entstehen im Bereich der Gerichte Dateien mit sensiblen persönlichen Daten, die den strengen gesetzlichen Vorgaben für entsprechende Datenverarbeitungen in der Verwaltung (beispielsweise des Bundeszentralregistergesetzes) entzogen sind? Werden die besonderen Geheimnisse, wie z. B. das Sozialgeheimnis und das Arztgeheimnis, auch dann ausreichend gewahrt, wenn entsprechende Vorgänge Gegenstand von gerichtlichen Verfahren und automatisiert gespeichert werden?

Für die Kontrolle in diesem Bereich ist der LfD nicht zuständig. Das LDatG bestimmt, daß dessen Kontrollzuständigkeit nur soweit reicht, wie die Gerichte verwaltend, nicht aber rechtsprechend tätig werden (§ 24 Abs. 1 LDatG).

Zweck dieser Regelung ist es, die verfassungsrechtlich verankerte richterliche Unabhängigkeit zu wahren. Alle Fragen, die den Inhalt der Rechtsprechung betreffen, sind der datenschutzrechtlichen Kontrolle – wie auch der Aufsicht durch die Justizverwaltung – entzogen. Im Gegenschluß ist der LfD der Auffassung, daß jede datenschutzrechtliche Frage, die durch die Justizverwaltung (das Justizministerium) geregelt wird oder entschieden werden kann, auch seiner datenschutzrechtlichen Kontrollzuständigkeit unterliegt. Die Grenzlinien sind in diesem Zusammenhang im Einzelfall schwierig zu ziehen.

7.1.2.1 Anmeldepflicht

Zweifelsfragen haben sich bereits bezüglich der Frage ergeben, ob der Einsatz von Personalcomputern im Bereich der Rechtsprechung durch Richter beim LfD gem. § 10 LDatG anzumelden ist. In diesem Zusammenhang hat die DSK folgende Auffassung vertreten:

Die in § 10 LDatG geregelte Anmeldepflicht betrifft auch die automatisierten Verfahren, die von Gerichten zu Zwecken der Rechtsprechung eingesetzt werden, da § 24 LDatG die Anwendung von § 10 LDatG nicht ausschließt.

Im Hinblick darauf, daß diese Anmeldungen grundsätzlich nicht konkret durch Datenschutzkontrollinstanzen kontrolliert werden könnten, und im Hinblick darauf, daß das Anmeldungsverfahren möglichst einheitlich und unkompliziert durchgeführt werden sollte, hat sich die DSK mit folgendem Kompromißvorschlag des Justizministeriums einverstanden erklärt: Danach teilt das Justizministerium der DSK bzw. dem LfD mit, bei welchen Gerichten welche Dezernate mit welchen dienstlichen Datenverarbeitungsgeräten ausgestattet werden. Es wird auch mitgeteilt, welche Programmprodukte den jeweiligen Dezernaten dienstlich zur Verfügung gestellt werden.

Die DSK ist davon ausgegangen, daß auch diese – gegenüber der in § 10 LDatG vorgesehenen Benachrichtigung eingeschränkte – Information ausreicht, um ihre Auskunftspflicht gegenüber den Bürgern (§ 11 LDatG) sowie ihre Berichts- und Beratungspflicht gegenüber dem Parlament (§ 22 LDatG) angemessen zu erfüllen. Diese Absprache wurde zwischenzeitlich durch die Übersendung einer entsprechenden Aufstellung über den Einsatz der EDV am Richterarbeitsplatz bestätigt und in die Tat umgesetzt.

7.1.2.2 Maßnahmen des technischen Datenschutzes

Unabhängig von der Frage, welche Stelle in welchem Umfang die Einhaltung datenschutzrechtlicher Anforderungen in diesem Bereich zu überwachen hat, ist es aus datenschutzrechtlicher Sicht sinnvoll, in Ergänzung der Dienstanweisung des Justizministeriums für die Benutzung von Personalcomputern zu dienstlichen Zwecken die betroffenen Richter auf folgendes hinzuweisen:

a) Die inhaltlichen Anforderungen des LDatG gelten auch für den Bereich, der der richterlichen Unabhängigkeit unterliegt; besonders bedeutsam sind in diesem Zusammenhang beispielsweise die Löschungspflichten, die insbesondere dann eingreifen, wenn die gespeicherten Daten zur Aufgabenerfüllung nicht mehr erforderlich sind (§ 13 Abs. 3 und 4 LDatG). Hinzuweisen ist auch auf den besonderen Auskunftsanspruch der betroffenen Bürger gem. § 12 LDatG.

b) Die Pflicht zur Realisierung von Maßnahmen zum technischen und organisatorischen Datenschutz trifft auch die speichernden Stellen, die der Rechtsprechung zuzurechnen sind (§ 9 Abs. 1 LDatG). Entsprechende Anforderungen sind nicht bereits durch Erlaß der o. g. allgemeinen Dienstanweisung des Justizministeriums als erfüllt anzusehen. Die technischen und organisatorischen Datenschutzanforderungen sind vielmehr auf der Ebene der speichernden Stelle selbst konkret umzusetzen sowie schriftlich festzulegen (§ 9 Abs. 2 LDatG).

Der LfD hat angeregt, die betroffenen Richter in geeigneter Form auf diese Gesichtspunkte hinzuweisen.

7.1.3 Pressemitteilungen von Justizbehörden

Es handelt sich nicht um Ausnahmefälle, wenn Betroffene sich an die Datenschutzkontrollinstitution wenden, weil etwa Pressesprecher von Staatsanwaltschaften zu Beginn von Ermittlungsverfahren Informationen in personenbezogener Form an die Presse weitergeben. Die DSK hatte insbesondere im Zusammenhang mit Straßenverkehrsdelikten Veranlassung, die Ermittlungsbehörden darauf hinzuweisen, daß Namensnennungen hier nur ausnahmsweise in Betracht kommen und daß auch sonstige Angaben, die zur Identifizierung des Betroffenen am Wohnort führen können, zurückhaltend weitergegeben werden sollten.

Dies entspricht den Richtlinien für die Tätigkeit der Justizpressestellen (vom 11. Mai 1965, JBl. S. 99), wo es heißt, daß Auskünfte nicht erteilt werden dürfen, wenn dadurch ein schutzwürdiges Interesse verletzt würde.

Mit einer nach Ansicht des Betroffenen unzutreffenden Darstellung eines Leitenden Oberstaatsanwalts aus Rheinland-Pfalz in einer Presseerklärung hat sich die Verwaltungsgerichtsbarkeit bis hin zum Bundesverwaltungsgericht befassen müssen. Dieses hat mit Beschluß vom 6. Februar 1991 (BVerwG 3 B 85/90) inhaltlich übereinstimmend mit dem OVG Koblenz (Urteil vom 20. März 1990, Az.: 7 A 101 aus 89), das wiederum mit dem erstinstanzlich ergangenen Verwaltungsgerichtsurteil im Ergebnis übereingestimmt hat, wie folgt entschieden:

Die Presseerklärung eines Leitenden Oberstaatsanwalts über das Ergebnis eines von seiner Behörde geführten Ermittlungsverfahrens ist mit Rücksicht auf den klagenden Beschuldigten rechtlich zu beanstanden, wenn sie den Behördenvorgang unzutreffend wiedergibt und den Kläger dadurch in seinem Persönlichkeitsrecht verletzt. Dabei ist auf den Eindruck abzustellen, den die Presseerklärung in der Öffentlichkeit erweckt.

Aus datenschutzrechtlicher Sicht ist diese Klarstellung zu begrüßen. Bedauerlich ist allerdings, daß es eines achtjährigen Rechtsstreites bedurfte, um dem betroffenen Bürger zur Durchsetzung seines Rechts auf Widerruf der behördlichen Behauptungen zu verhelfen.

7.1.4 Aktenübersendungen zwischen Gerichten

Im 12. Tätigkeitsbericht der DSK wurde dargestellt, daß es zwischen Arbeits- und Sozialgerichten zu einer Kontroverse über die Frage gekommen ist, in welchem Umfang eine Verpflichtung der Arbeitsgerichte besteht, auf Anforderung der Sozialgerichte ganze Prozeßakten an die Sozialgerichte zu übersenden, und ob die um die Aktenübersendung ersuchten Arbeitsgerichte ein eigenständiges Prüfungsrecht haben, damit ggf. Teile der Prozeßakten oder der Beiakten von der Übersendung ausgenommen werden könnten.

Die DSK hat in ihrem 12. Tätigkeitsbericht (Tz. 7.2.3) die Auffassung des Justizministeriums wiedergegeben, daß ein solches eigenständiges Prüfungsrecht des ersuchten Gerichts nicht existiere, da dieses in der Praxis zu unüberwindbaren Schwierigkeiten führen müsse und zudem die Entscheidungskompetenz auf das ersuchte Gericht verlagert würde, ohne daß dies rechtlich geboten wäre.

Nunmehr ist die Angelegenheit unter datenschutzrechtlichen Gesichtspunkten zufriedenstellend bereinigt worden:

Zwischen allen beteiligten Stellen besteht jetzt darüber Einigkeit, daß die ersuchte Stelle grundsätzlich ein eigenes – wenn auch eingeschränktes – Prüfungsrecht bezüglich der Erforderlichkeit der zu übersendenden Akten für die Zwecke der anfordernden Stelle besitzt. Dieses Prüfungsrecht bezieht sich insbesondere auf die Eignung der angeforderten Akten für den angegebenen Zweck.

Aus der Sicht des LfD ist es erforderlich, daß die aktenanfordernden Stellen ihr Begehren möglichst genau nach dem Zweck und nach Art und Inhalt der angeforderten Akten bezeichnen. Wenn dabei oft auch nur pauschale Angaben gemacht werden können, so sollte nach Auffassung des LfD das Justizministerium jedenfalls darauf hinwirken, daß entsprechende Aktenübersendungsgesuche soweit wie möglich konkretisiert werden.

7.2 Zivilgerichtsbarkeit; Veröffentlichung von Schuldnerdaten in Zwangsversteigerungsverfahren

Im Rahmen von Zwangsversteigerungsverfahren von Grundstücken werden die entsprechenden Terminankündigungen in der Tagespresse und an der Gerichtstafel unter Nennung von Namen und Anschriften von Schuldnern bzw. Grundstückseigentümern veröffentlicht.

Ein Beschwerdeführer schilderte, daß ein Schuldner in seiner Tageszeitung mit folgender Anschrift bezeichnet worden sei: „Zur Zeit JVA Koblenz-Karthause".

In diesem Zusammenhang ist ein wirksamer Schutz der Betroffenen durch gerichtliche Rechtsmittel kaum zu erreichen; obergerichtlicher Rechtsprechung zufolge kann auch bei einem möglich erscheinenden Grundrechtsverstoß durch die Terminbestimmung kein Rechtsmittel gegen die insoweit erfolgende Verfahrensweise in Anspruch genommen werden (Beschluß des OLG Zweibrücken vom 21. Mai 1987, NJW 87, S. 2590).

Die DSK hat deshalb das Justizministerium um Prüfung gebeten, ob nicht durch allgemeine Hinweise an die tätig werdenden Gerichte (Rechtspfleger) bewirkt werden kann, daß auf die Veröffentlichung zumindest von Teilen der die Betroffenen identifizierenden Merkmale verzichtet werden kann; in Betracht käme etwa ein Verzicht auf die Angabe der genauen Wohnanschrift. Möglicherweise würde es ausreichen, den Wohnort anzugeben.

Das Justizministerium hat wie folgt Stellung genommen:

- Bei der Veröffentlichung in der Tageszeitung mit Angabe der Anschrift „zur Zeit JVA" habe es sich um ein bedauerliches Versehen gehandelt, das auf eine seinerzeitige vertretungsweise bedingte Überlastung des zuständigen Beamten zurückzuführen sei. Bei zusätzlichen Veröffentlichungen von Terminbestimmungen in der Tageszeitung werde der Name der eingetragenen Eigentümer ansonsten grundsätzlich nicht angegeben.

- Für die Bekanntgabe an der Gerichtstafel sei eine genaue Bezeichnung des Eigentümers und des Schuldners zulässig, wenn nicht sogar gesetzlich gefordert. Auch eine entsprechende Veröffentlichung in Tageszeitungen könne nicht als rechtlich unzulässig bezeichnet werden.

Das Justizministerium hat jedoch die Präsidenten der Oberlandesgerichte darum gebeten, in einer ihnen als geeignet erscheinenden Weise dafür Sorge zu tragen, daß die befaßten Gerichte in diesen Fällen auf den Persönlichkeitsschutz des Schuldners Bedacht nehmen mögen. Dies ist aus Sicht des LfD zu begrüßen. Eine entsprechende Verfahrensweise ist nicht nur wünschenswert, sondern verfassungsrechtlich zwingend geboten. Das Gesetzesrecht ist insoweit verfassungskonform auszulegen.

7.3 Strafverfahren

7.3.1 Gesetzgebungsvorhaben

Es ist ein seit langem bestehendes Anliegen der Datenschutzbeauftragten, das informationelle Selbstbestimmungsrecht der Betroffenen in Strafverfahren durch eine Ergänzung der Strafprozeßordnung deutlich und eng am Verhältnismäßigkeitsgrundsatz orientiert zu regeln.

Dem sollte ein Gesetzentwurf dienen, der als „Strafverfahrensänderungsgesetz" (StVÄG) durch das Bundesjustizministerium erstellt wurde. Dieses Vorhaben befindet sich immer noch im Stadium des Referentenentwurfs. Zu den dort vorgeschlagenen Regelungen haben die Datenschutzbeauftragten ausführlich Stellung genommen (vgl. 12. Tb der DSK, Tz.7.3.4 und Anlage 4 zum 12. Tb).

Diese grundlegende Revision der Strafprozeßordnung ist durch Bestrebungen überholt worden, den Strafverfolgungsbehörden im Bereich der Bekämpfung der organisierten Kriminalität und der Rauschgiftkriminalität besondere Ermittlungsbefugnisse zu geben. Diese besonderen Befugnisse sollten Teil eines sogenannten Gesetzes zur Bekämpfung der organisierten Kriminalität sowie der Rauschgiftkriminalität werden. Die aus Sicht der Datenschutzbeauftragten hierzu bedeutsamen Überlegungen sind in einem Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zusammengefaßt, der im Anhang (Anlage 4) abgedruckt wird.

Ein weiteres Gesetzgebungsvorhaben im Bereich der Strafprozeßordnung ist zwischenzeitlich in Kraft getreten: Das Gesetz zur Stärkung des Opferschutzes im Strafverfahren. Teil dieses Gesetzes ist eine Erweiterung der Möglichkeiten, die Öffentlichkeit im Interesse des Opferschutzes aus dem Strafverfahren auszuschließen. Ob dies in der Praxis häufig genutzt wird, ist fraglich; eine Verletzung der Vorschriften über die Öffentlichkeit zu Lasten des Angeklagten ist als sog. „absoluter Revisionsgrund" anzusehen (§ 338 Nr. 6 StPO). Dies mag zur Zurückhaltung der gerichtlichen Praxis bei der Nutzung der genannten Möglichkeiten beitragen. Der LfD hat gegenüber dem Justizministerium angeregt, weitere Bestrebungen zu unternehmen, um durch eine Begrenzung des Grundsatzes der Öffentlichkeit die Persönlichkeitsrechte von Zeugen und Opfern im Gerichtsverfahren zu schützen.

7.3.2 Geschäftsstellenautomation der Staatsanwaltschaften

Im 12. Tätigkeitsbericht wurde der Einsatz des Geschäftsstellenautomationssystems „GAST" bei den Staatsanwaltschaften Mainz und Zweibrücken dargestellt. Die bestehenden datenschutzrechtlichen Schwachpunkte dieses Verfahrens wurden ebenfalls geschildert. Die DSK hatte um Abhilfe dieser Verstöße gegen die Anforderungen des technischen und organisatorischen Datenschutzes gebeten. Das Justizministerium hat daraufhin mitgeteilt, daß daran gedacht sei, das gesamte System GAST zu ersetzen, und daß es wirtschaftlich unvertretbar sei, Änderungen durchzuführen, die nur noch für eine Übergangszeit von rund zwei Jahren wirksam wären.

Vor diesem Hintergrund hat die DSK die aus datenschutzrechtlicher Sicht wichtigsten Defizite des zur Zeit eingesetzten Systems benannt und um eine genaue Quantifizierung des zu deren Beseitigung erforderlichen Programmänderungsaufwandes gebeten.

Das Justizministerium hat den erforderlichen Änderungsaufwand nicht beziffert, es hat vielmehr bestätigt, daß jede Änderung am GAST-Verfahren aus wirtschaftlichen Gründen abgelehnt werde.

Die DSK hat dies bedauert und festgestellt, daß das zur Zeit bei den Staatsanwaltschaften Mainz und Zweibrücken eingesetzte Verfahren den datenschutzrechtlichen Anforderungen nicht entspricht.

Zur Zeit stellt sich die Situation wie folgt dar:

Das Justizministerium hat die Entwicklung eines neuen Geschäftsstellenautomationssystems der Staatsanwaltschaften in Auftrag gegeben. Damit soll vor allem eine Integration der erforderlichen Textverarbeitung bei den Staatsanwaltschaften mit der dort erfolgenden Registerführung möglich werden. Das neue System nennt sich „Computer-Unterstützung der Staatsanwaltschaften Rheinland-Pfalz", CUST.

Dieses System wird in mehreren Teilstufen unter Einbindung des Schreibdienstes realisiert. Aus datenschutzrechtlicher Sicht ist dabei wesentlich, daß eine Vernetzung der Datenverarbeitungssysteme zwischen den verschiedenen Staatsanwaltschaften nicht geplant ist, m. a. W., daß jede Staatsanwaltschaft nur die bei ihr erfaßten und entstandenen Informationen automatisiert abrufen kann.

Das Justizministerium hat den LfD bisher noch nicht über den Beginn des Echtbetriebes dieses Systems in Kenntnis gesetzt. Er wird unmittelbar nach einer entsprechenden Mitteilung örtliche Feststellungen veranlassen. Sein Hauptaugenmerk wird dabei auf folgenden Gesichtspunkten liegen:

- Bei den in einem Geschäftsstellenautomationssystem der Staatsanwaltschaften gespeicherten Daten handelt es sich um sensible Informationen. Ihrer Richtigkeit kommt besondere Bedeutung zu. Hierfür muß die Verantwortung des Staatsanwalts eindeutig geregelt werden. Bei ihren abschließenden Verfügungen muß die Fortschreibung und Korrektur der automatisiert zu speichernden Datensätze veranlaßt werden.

- Eine Speicherung von Fällen, in denen noch nicht einmal die Schwelle des „Anfangsverdachts" im Sinne der Strafprozeßordnung überschritten wurde, ist grundsätzlich nicht zulässig.

- Opferdaten sollten grundsätzlich nicht im automatisierten System gespeichert werden.

- Die Dauer der automatisierten Speicherung darf sich nicht an den Aufbewahrungsbestimmungen für die Justizakten orientieren; maßgeblich ist vielmehr allein der Erforderlichkeitsgrundsatz des § 13 LDatG.

- Auch innerhalb der Staatsanwaltschaften sind Zugriffsbeschränkungen entsprechend den geltenden internen Zuständigkeitsabgrenzungen einzurichten.

7.3.3 Automatisierte Unterstützung von Ermittlungsverfahren

Einer Anmeldung entnahm der LfD, daß ein Polizeipräsidium in zwei Fällen die Auswertung von abgehörten Telefonaten mit Hilfe eines Personalcomputers durchführt, und daß das Justizministerium hier die Staatsanwaltschaft als speichernde Stelle ansieht, mit der Folge, daß die eigentlich tätig werdende Polizei nur als Auftragnehmer in einem Verhältnis der Auftragsdatenverarbeitung betrachtet wird (zu den spezifischen Problemen der Verwertung von Erkenntnissen aus abgehörten Telefonaten s. o. Tz. 5.5).

In der Vergangenheit waren alle beteiligten Stellen davon ausgegangen, daß Datenspeicherungen durch Polizeidienststellen auch im repressiven Bereich nicht als Fall der datenschutzrechtlichen Auftragsdatenverarbeitung für die jeweilige Staatsanwaltschaft anzusehen sind.

Die gegenteilige Ansicht hat jedoch – nach den beim LfD vorliegenden Erfahrungen – weder in bezug auf die materiellen Anforderungen an die Datenverarbeitung noch bezüglich der Kontrollkompetenz des LfD praktische Änderungen zur Folge. Es könnte deshalb auf eine weitere Diskussion dieser Frage mit dem Ziel der Klärung und Herstellung von Konsens verzichtet werden, wenn bezüglich folgender Punkte Übereinstimmung besteht:

- Wenn Auftraggeber wie Auftragnehmer nichtrichterliche öffentliche Stellen des Landes Rheinland-Pfalz (gem. § 2 Abs. 1 LDatG) sind, unterliegen beide Stellen den Anforderungen des LDatG. Auch Prüfungsmaßnahmen des LfD sind gegenüber beiden Stellen möglich (§ 4 LDatG; vgl. auch Nr. 4 der Verwaltungsvorschrift zur Durchführung des LDatG).

- Wenn auch in den Fällen, in denen die Staatsanwaltschaft als Auftraggeber und damit als speichernde Stelle im Sinne des LDatG angesehen wird, für die Modalitäten der Datenverarbeitung durch den Auftragnehmer (die Polizei) eine Errichtungsanordnung erlassen wird, wie dies im Polizeibereich generell erfolgt. Diese Errichtungsanordnungen erfüllen die Funktion einer Dienstanweisung gemäß § 9 Abs. 2 LDatG; sie enthalten also unmittelbare Anweisungen an die datenverarbeitende Stelle. Die üblicherweise dort enthaltenen Festlegungen haben sich als zweckmäßig erwiesen. Auch das Anmeldeverfahren könnte in Anlehnung an die bisherige durch die Polizeidienststellen bzw. das Ministerium des Innern praktizierte Verfahrensweise vereinfacht werden: Unter Verzicht auf eine Ausfüllung des Formblatts DSR 1 könnte dem LfD mit einem kurzen Anschreiben die Errichtungsanordnung vorgelegt werden, wenn sich aus dieser die zur Information des LfD wesentlichen Daten ergeben.

Das Justizministerium hat sein Einverständnis hierzu erklärt.

7.3.4 Ärztebetrugsverfahren

Angesichts der nach wie vor großen Zahl von Ermittlungsverfahren gegen Ärzte, von denen insbesondere auch Patienten als Zeugen betroffen sind, hat der LfD es für angemessen gehalten, alle an diesen Ermittlungsverfahren beteiligten Personen und Behörden auf die in diesem Zusammenhang zu beachtenden Grundsätze des Persönlichkeitsschutzes der Patienten hinzuweisen. Dies erfolgte durch die Veröffentlichung und gezielte Verbreitung der folgenden Hinweise:

7.3.4.1 Allgemeine Grundsätze für den Umgang mit Patientendaten in Ermittlungsverfahren gegen Ärzte

Allen Behörden, die – insbesondere gegen Ärzte gerichtet – wegen Betrugsstraftaten im Gesundheitsbereich ermitteln, muß bewußt sein, daß die den Gesundheitszustand der Patienten und die ihre Behandlung betreffenden Informationen einem besonderen, verfassungsrechtlichen Schutz unterliegen. Die Geheimhaltungsinteressen des einzelnen treten nur dann und insoweit zurück, wie überwiegende Belange des Gemeinwohls dies zwingend gebieten. Es kommt entscheidend – hier wie auch in anderen Zusammenhängen – darauf an, ob der Eingriff in die Privatsphäre des Bürgers bei einer Abwägung, die alle Umstände des Einzelfalles in Betracht zieht, dem Verhältnismäßigkeitsgrundsatz entspricht (Bundesverfassungsgericht, Beschluß zur Beschlagnahme der ärztlichen Karteikarte eines Beschuldigten vom 8. März 1972, NJW 72, S. 1123, 1124).

Zu den Belangen des Gemeinwohls, die für eine Beschlagnahme sprechen, zählt insbesondere der staatliche Strafanspruch im Zusammenhang mit dem Rechtsstaatsprinzip (woraus die grundsätzlich bestehende Pflicht des Staates folgt, möglichst umfassend die Wahrheit über begangene Straftaten zu ermitteln; vgl. Bundesverfassungsgericht, Beschluß zur Beschlagnahme von Pressematerial – ZDF –, BVerfGE 71, 252). Bei Eingriffen in das informationelle Selbstbestimmungsrecht der Patienten ist nicht ohne Bedeutung, ob und inwieweit eine tatsächliche Gewähr dafür gegeben ist, daß das Wissen um die grundsätzlich der ärztlichen Schweigepflicht unterfallenden Tatsachen – ggf. durch Erörterung in nichtöffentlicher Verhandlung – auf den Kreis der unmittelbar am Verfahren Beteiligten beschränkt werden kann (so wörtlich das Bundesverfassungsgericht im zitierten Patientenkarteikarten-Beschluß).

7.3.4.2 Verhältnismäßigkeitsgrundsatz bei der Datenerhebung

a) Beschränkungen bei Beschlagnahmen

Soweit Informationen im Rahmen von Abrechnungsbetrugsverfahren durch die Beschlagnahme von Patientenkarteikarten bei den Ärzten erhoben werden, gebietet der Verhältnismäßigkeitsgrundsatz prinzipiell, lediglich Auswahlmengen (Stichproben) aus der Patientenkartei des beschuldigten Arztes zu beschlagnahmen, sofern der jeweilige Fall dafür geeignet ist. Darüber hinausgehende konkrete Ermittlungshandlungen sind angesichts der Vielfältigkeit der möglichen Fallgestaltungen selbstverständlich nicht ausgeschlossen.

b) Schonungsprinzip bei Vernehmungen

Soweit personenbezogene Daten der betroffenen Patienten bzw. Patientinnen erhoben werden, gebietet der Verhältnismäßigkeitsgrundsatz, nur diejenigen Fragen zu stellen und nur die Informationen in Akten oder in sonstiger Weise zu speichern, die für das Strafverfahren gegen den beschuldigten Arzt von Bedeutung sein können. Soweit Fragen gestellt werden müssen, die eine mögliche Strafbarkeit des Zeugen betreffen (z. B. nach begangenen Abtreibungen), ist der Zeuge vorher auf sein Auskunftsverweigerungsrecht (§ 55 StPO) hinzuweisen.

Fragen nach Tatsachen, die dem Zeugen oder der Zeugin zur Unehre gereichen können oder deren persönlichen Lebensbereich (also insbesondere auch Gesundheitsdaten) betreffen, sollen nur gestellt werden, wenn es für Zwecke des Strafverfahrens unerläßlich ist (s. a. § 68 a Abs. 1 StPO). Dies ist beispielsweise bezüglich der Behandlungsmaßnahmen von Frauenärzten oder Psychiatern von besonderer Bedeutung.

Bei der Vernehmung ist außerdem darauf zu achten, daß dem Zeugen nicht Informationen offenbart werden, die der Arzt dem Patienten aus Gründen des Gesundheitsschutzes nicht bekanntgegeben hat.

Es ist zu ermöglichen, daß Patientinnen – insbesondere bei Ermittlungen gegen Frauenärzte – durch weibliche Vernehmungspersonen befragt werden.

7.3.4.3 Maßnahmen des technischen und organisatorischen Datenschutzes

Die dem Patientengeheimnis unterliegenden erhobenen Informationen dürfen nur dem Kreis der unmittelbar am Verfahren Beteiligten zugänglich gemacht werden; nur durch diese darf eine Nutzung erfolgen, die strikt auf Strafverfolgungszwecke zu beschränken ist. Unter diesem Gesichtspunkt sind die Vorschriften der Richtlinien über das Straf- und Bußgeldverfahren (RiStBV) über Akteneinsicht und Auskunftserteilungen aus Akten restriktiv auszulegen, soweit dem Patientengeheimnis unterliegende Informationen in den Akten von Einsichts- oder Auskunftsansprüchen Dritter betroffen sind.

Soweit Personen, die nicht Bedienstete der Ermittlungsbehörden sind, bei den Vernehmungen im Ermittlungsverfahren anwesend sind (z. B. als Sachverständige), muß gewährleistet sein, daß sie entweder als Amtsträger oder wie Amtsträger zur Verschwiegenheit verpflichtet sind und der gleichen Strafandrohung unterliegen (erforderlichenfalls durch Verpflichtung nach dem Verpflichtungsgesetz).

Es müssen angemessene Formen der Datensicherung für die dem Patientengeheimnis unterliegenden Informationen bzw. die entsprechenden Datenträger (Akten u. ä.) vorhanden sein. Beschlagnahmte Patientenunterlagen sollten beispielsweise in eigens bereitgestellten Räumen gelagert und bearbeitet werden. Falls dies aus tatsächlichen Gründen nicht möglich ist, sollten die auch anderen Zwecken dienenden Räume jedenfalls besonders gesichert werden können. Durch entsprechende Maßnahmen muß sichergestellt sein, daß nur die zuständigen Sachbearbeiter Zugang haben.

Kopien dürfen nur im erforderlichen Umfang und in einem kontrollierten Verfahren erstellt werden. Es muß außerdem sichergestellt sein, daß sie kontrolliert und unter Ausschluß des Zugriffs Dritter (externer Stellen) vernichtet werden.

7.3.5 Datenübermittlungen durch Staatsanwaltschaften

Wiederholt war der LfD aufgrund von Eingaben mit der Frage befaßt, unter welchen Voraussetzungen welche Daten aus Strafakten an andere Stellen übermittelt werden dürfen.

So hat in einem Fall eine Staatsanwaltschaft die gesamten Strafakten aus einem abgeschlossenen Verfahren wegen Betäubungsmittelmißbrauchs an eine private Versicherung übersandt, obwohl diese Versicherung in ihrem Anforderungsschreiben keinen Hinweis darauf gegeben hat, zu welchem Zweck sie diese Akten benötigt. Nach den hier vorliegenden Erkenntnissen war Zweck des Akteneinsichtsbegehrens die Prüfung eines privatrechtlichen Versicherungsfalles, der in keinem Zusammenhang mit der Straftat (Rauschgiftdelikt) stand. Dann aber ist eine entsprechende Aktenübersendung unzulässig, auch wenn sich die private Versicherung eines Rechtsanwaltes bedient. Darauf und auf die Pflicht, eine Prüfung der durch Verwaltungsvorschrift (Nr. 183 RiStBV) vorgeschriebenen Übermittlungsvoraussetzungen auch tatsächlich durchzuführen, hat der LfD die betroffene Staatsanwaltschaft hingewiesen.

In einem anderen Fall hat der zuständige Staatsanwalt eine Ermittlungsakte in vollem Umfang an das zuständige Finanzamt des Beschuldigten übersandt, um eine Überprüfung zu veranlassen.

Das Finanzamt konnte dem Sachverhalt keinen steuerrechtlich relevanten Tatbestand entnehmen, es hat aber die Information über die Vorstrafen des Beschuldigten, die in der Strafakte enthalten waren, dazu genutzt, um einige Jahre später die Ablehnung einer steuerrechtlichen Beschwerde des Beschuldigten in ganz anderem Zusammenhang ergänzend zu begründen.

Auch hier ist der LfD der Auffassung, daß die umfassende Information der Finanzbehörde durch Übersendung der gesamten Strafakte, in der zudem die Anklageschrift aus einem ganz anderen Verfahren in Kopie enthalten war, nicht erforderlich war, wenn eine Beschränkung auf Aktenteile, die die finanzielle Situation und die Einkünfte des Betroffenen zum Gegenstand hatten, zur Prüfung für steuerliche und steuerstrafrechtliche Zwecke ausgereicht hätte. Insbesondere die Weitergabe von Informationen über Vorstrafen, die im Bundeszentralregister bereits gelöscht sind, ist nur in Ausnahmefällen erforderlich. Angesichts der Sensitivität der Inhalte strafrechtlicher Ermittlungsakten (die das soziale Umfeld und auch Daten Dritter betreffen) ist generell eine zurückhaltende Vorgehensweise bei Aktenübermittlungen geboten. Eine abschließende Beurteilung des geschilderten konkreten Falles aus datenschutzrechtlicher Sicht ist dem LfD derzeit jedoch noch nicht möglich, weil die zuständige Staatsanwaltschaft ihm die abgeschlossenen Strafakten noch nicht zur Verfügung gestellt hat.

Aus datenschutzrechtlicher Sicht war allerdings auch zu bemängeln, daß erforderliche Datenübermittlungen unterblieben sind:

Die DSK hat in ihren vorangegangenen Tätigkeitsberichten (zuletzt im 12. Tb., Tz.7.3.5) wiederholt darauf hingewiesen, wie bedeutsam es ist, daß die Staatsanwaltschaften die betroffenen Polizeidienststellen über das Ergebnis der Strafverfahren unterrichten. Nur dann kann die Polizei ihre Datensammlungen aktualisieren und durch vorgeschriebene Löschungen bereinigen. Nur dann kann die Polizei auch von zutreffenden Tatsachengrundlagen bei ihrer sonstigen Tätigkeit ausgehen. Die Konferenz der DSB hat wegen der vordringlichen Bedeutung dieser Frage bereits 1987 einen gesonderten Beschluß hierzu gefaßt (vom 4. Mai 1987, Anlage 3 zum 11.Tb der DSK).
Bei einer stichprobenartigen Überprüfung von 100 Strafakten wurde bei einer Staatsanwaltschaft des Landes festgestellt, daß in drei Fällen entsprechende Übermittlungen nicht erfolgt sind. Welche Bedeutung diese Rückmeldungen haben, wurde bereits oben unter Tz. 5.2 ausführlich unter Zugrundelegung eines konkreten Falles geschildert.
Die DSK und der LfD haben sich darum bemüht, das Justizministerium zu veranlassen, hier durch verstärkte Kontrollmaßnahmen und Hinweise an die betroffenen Bediensteten für Abhilfe zu sorgen. Außerdem sollte durch eine erweiternde Auslegung der diese Übermittlung regelnden Vorschrift (Nr.11 MiStra) sichergestellt werden, daß eine solche Rückmeldung in jedem Fall erfolgt, in dem eine Speicherung von Ermittlungsdaten im polizeilichen Informationssystem „POLIS" vorliegt. Zum Teil sind diese Vorschläge vom Justizministerium aufgegriffen worden. Der LfD geht davon aus, daß die Fehlerquote aufgrund der Aufmerksamkeit, die diese Vorgänge nunmehr finden, geringer wird.

7.3.6 Nennung von Zeugenanschriften im Strafbefehl

Auf den formularmäßig gestalteten Strafbefehlen wird regelmäßig der Name sowie die genaue Anschrift (Wohnort und Straße) des oder der Zeugen angegeben. Dies kann schutzwürdige Belange der betroffenen Zeugen berühren, wenn nicht auszuschließen ist, daß der Beschuldigte dem Zeugen gegenüber nachteilige Handlungen (noch am harmlosesten in diesem Zusammenhang wären telefonische Belästigungen) verübt.

Die DSK hat die Auffassung vertreten, daß es nach dem Wortlaut der Strafprozeßordnung (die nur von Angabe des „Wohnortes" spricht) nicht zweifelsfrei geboten ist, die genaue Wohnanschrift zu benennen. In der Literatur ist diese Frage umstritten. Das Ministerium der Justiz ist in verschiedenen Zusammenhängen jedenfalls selbst der Auffassung, daß die Begriffe „Wohnort" und „genaue Anschrift" eine unterschiedliche Bedeutung haben.

Die DSK hat das Ministerium der Justiz darum gebeten, Überlegungen anzustellen, das Spannungsverhältnis zwischen Zeugenschutz und Aufklärungsbedürfnis durch eine differenzierende Regelung aufzulösen, so daß im Regelfall zunächst auf dem Strafbefehl nur der Wohnort des Zeugen, nicht dagegen seine genaue Anschrift genannt wird. In diesem Sinne haben sich auch die staatsanwaltschaftliche Praxis des Landes Bremen sowie das Justizministerium des Landes Niedersachsen ausgesprochen.

Das rheinland-pfälzische Justizministerium hat sich diesen Überlegungen leider verschlossen und unter bloßer Berufung auf den gesetzlichen Wortlaut jede weitere Überlegung in diesem Zusammenhang abgelehnt. Der LfD wird in dieser Frage weiterhin um eine datenschutzgerechtere Lösung bemüht sein. Zu vergleichbaren Fragen in Ordnungswidrigkeitenverfahren s. oben Tz. 5.3 .

7.3.7 Fazit

Die vorgenannten Fälle zeigen, daß Datenschutz und die Kontrolle der Datenverarbeitung durch eine unabhängige Behörde gerade auch im Bereich der staatsanwaltschaftlichen Tätigkeit eigenständige Bedeutung haben. Diese Bedeutung liegt hier – wie auch in anderen Bereichen staatlichen Handelns – nicht zuletzt darin, daß die Tätigkeit des LfD dazu beitragen kann, Mißtrauen in den staatlichen Umgang mit höchstpersönlichen Informationen abzubauen und an einem Klima des Vertrauens zwischen Bürgern und staatlichen Einrichtungen mitzuwirken, ohne das ein effizientes Handeln auch für die Justiz nicht möglich ist (vgl. die Ausführungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil zur Bedeutung vertrauensbildender Maßnahmen für staatliches Handeln, B II 2 b bb am Ende). Der Grundsatz, daß angesichts der Undurchsichtigkeit von Datenverarbeitungsmaßnahmen im Zeitalter der automatisierten Datenverarbeitung ein vorgezogener Rechtsschutz der Bürger durch rechtzeitige Vorkehrungen zu erfolgen hat und daß ein wesentlicher Teil dieser Maßnahmen die Kontrolle durch Datenschutzbeauftragte ist (vgl. Beschluß des BVerfG vom 20. Juni 1984, 1 BvR 1494/78, B IV 4), gilt auch hier. In Anbetracht der Tatsache, daß die Eingriffsbefugnisse der Staatsanwaltschaft zur Informationsgewinnung sehr weitreichend sind, daß durchaus nicht jede Maßnahme in diesem Zusammenhang gerichtlich überprüft wird, daß unbeteiligte Dritte (etwa als Zeugen) betroffen sind und daß auch unter quantitativen Gesichtspunkten die Informationsgewinnung der Staatsanwaltschaften bedeutsam ist, ist eine funktionsfähige Datenschutzkontrolle in diesem Bereich unerläßlich.

7.4 Strafvollzug

Selbstverständlich sind Gefangene Grundrechtsträger; Beschränkungen ihres informationellen Selbstbestimmungsrechtes dürfen – grundsätzlich nicht anders als bei anderen Bürgern – nur aufgrund eines Gesetzes erfolgen, das den Erfordernissen der Verhältnismäßigkeit und Normenklarheit entspricht.

Das Strafvollzugsgesetz enthält derzeit kaum datenschutzrechtliche Regelungen. Die Bemühungen des Bundesministers der Justiz zur Novellierung des Strafvollzugsgesetzes sind bisher an den unterschiedlichen Vorstellungen der Landesjustizverwaltungen gescheitert. In einer Reihe von Verwaltungsvorschriften (z. B. Strafvollstreckungsordnung, Vollzugsgeschäftsordnung, Richtlininen zum Jugendgerichtsgesetz, Richtlinien zum Straf- und Bußgeldverfahren) haben die Justizverwaltungen unter anderem auch datenschutzrechtlich relevante Regelungen getroffen. Im Hinblick auf das Volkszählungsurteil des Bundesverfassungsgerichts sind jedoch zumindest grundsätzliche Fragen der Datenverarbeitung durch Justizvollzugsanstalten in einem Gesetz oder in einer Rechtsverordnung zu regeln. Weiterhin erfordern die Automationsabsichten der Justiz im Strafvollzugsbereich Datenschutzregelungen, insbesondere zu folgenden Fragen: Umfang der Datenerhebung und -speicherung, spezifische Übermittlungsvorschriften, Sicherung und Löschung der erhobenen Daten, Rechte der Betroffenen, insbesondere Auskunftsansprüche. Der LfD hat deshalb – fußend auf Arbeiten des Arbeitskreises Justiz der Datenschutzbeauftragten des Bundes und der Länder – seine datenschutzrechtlichen Anliegen in diesem Bereich in einer umfassenderen Darstellung zusammengefaßt und dem Justizministerium mit der Bitte um Stellungnahme übersandt. Das entsprechende Papier ist als Anlage 7 zu diesem Tb abgedruckt.

7.5 Schuldnerverzeichnis

Im 12. Tätigkeitsbericht der DSK (Tz. 7.5.2) wurde ausführlich geschildert, welche Gefahren aus datenschutzrechtlicher Sicht auch für unbeteiligte Dritte mit Auskünften aus dem Schuldnerverzeichnis verbunden sind.

Um Anhaltspunkte dafür zu gewinnen, ob und ggf. wie in der Praxis diesen Gefahren entgegengewirkt werden kann, hat die DSK örtliche Feststellungen beim Schuldnerverzeichnis eines großen Amtsgerichts durchgeführt. Als Ergebnis wurde festgestellt:

a) Allgemeines

Das Verfahren wird regelmäßig dadurch eingeleitet, daß ein Gläubiger unter Beifügung eines Titels und einer Fruchtlosigkeitsbescheinigung die Abgabe der eidesstattlichen Versicherung beantragt. Falls der Schuldner zum Termin nicht erscheint, wird auf Antrag des Gläubigers ein Haftbefehl erlassen und auf weiteren Antrag des Gläubigers auch vollstreckt. Mit Abgabe der eidesstattlichen Versicherung bzw. mit Erlaß eines Haftbefehls erfolgt die Eintragung in das Schuldnerverzeichnis. Jährlich werden Karteikarten unterschiedlicher Farbe angelegt, in die alle Verfahren eingetragen werden, die bezüglich des betreffenden Schuldners durchgeführt werden. Immer dann, wenn die eidesstattliche Versicherung abgelegt wird, werden das Geburtsdatum und der Geburtsort eingetragen, so daß diese Informationen dann vorhanden sind. Auch in den Fällen, in denen der Gläubiger diese Angaben liefert, werden sie in die Karteikarte eingetragen. Die Eintragung der Wohnanschrift beruht nur auf Angaben des Gläubigers. In den zahlreichen Fällen, in denen der Gläubiger keine Angaben zum Geburtsdatum macht und der Schuldner nicht zur Abgabe der eidesstattlichen Versicherung erscheint, fehlt das Geburtsdatum.

b) Zur Auskunftserteilung

Grundsätzlich werden schriftliche Anfragen so beantwortet, daß die Anfrage urschriftlich mit einem Stempelvermerk versehen zurückgesandt wird. Dieser Stempelvermerk sieht folgende Angaben vor: – Kein Eintrag im Schuldnerverzeichnis – Schuldner hat am xy in 11/24 M xy die eidesstattliche Versicherung abgegeben. – Es liegt/liegen xy Haftbefehle vor. Geschäftsstelle des Amtsgerichts, den ...

Im Regelfall verbleiben über entsprechende Anfragen keine Unterlagen mehr beim Amtsgericht. Ausnahmen gelten dann, wenn mit der Anfrage ein Titel übersandt wird. Dann erfolgt die Beantwortung durch Formblatt, die Anfrage selbst wird in eine Akte aufgenommen und die Rücksendung des Titels aktenkundig gemacht.

c) Löschung der Eintragungen

Die Eintragungen werden auf Antrag des Schuldners gelöscht, wenn er nachweist, daß er den Gläubiger befriedigt hat und wenn drei Jahre nach Ablauf der eidesstattlichen Versicherung vergangen sind, und von Amts wegen, wenn fünf Jahre nach Abgabe der eidesstattlichen Versicherung vergangen sind.

Die regelmäßigen Aussonderungsarbeiten werden in der Form durchgeführt, daß zu Beginn eines Jahres die von Amts wegen zu löschenden Informationen durch Entnehmen der entsprechenden farbigen Karteikarten aus der Kartei entfernt werden. Diese Karteikarten werden vernichtet.

d) Zur Statistik

Monatlich werden ca. vier- bis fünfhundert Auskünfte aus dem Schuldnerverzeichnis erteilt. Die Hälfte davon etwa ist an private Gläubiger gerichtet, die andere Hälfte betrifft Auskünfte an die Ausländerbehörde oder sonstige kommunale Stellen.

e) Regelmäßige Informationsübermittlungen

Zur regelmäßigen Datenübermittlung aus dem Schuldnerverzeichnis werden maschinenschriftliche Listen gefertigt, in denen Angaben zur Identität der Schuldner sowie zum Eintragungsgrund in das Schuldnerverzeichnis (eidesstattliche Versicherung, Haftbefehl) gemacht werden. Empfänger dieser Listen sind die Industrie- und Handelskammer, die Schufa GmbH sowie zwei Auskunfteien. Die letzteren erhalten aufgrund einer ausdrücklichen Genehmigung des Landgerichtspräsidenten die entsprechenden Listen. Die Datenübermittlung ist gebührenpflichtig, die Gebühr beträgt pro Mitteilung (Schuldner) 0,15 DM.

Es ist deutlich geworden, daß auch unmittelbare Auskünfte aus dem Schuldnerverzeichnis und Listenübersendungen hieraus eine große Rolle spielen. Aus datenschutzrechtlicher Sicht ist deshalb anzustreben, daß insbesondere die Verwechslungsgefahr minimiert wird, die sich auch im Berichtszeitraum wieder bestätigt hat: Erneut waren Eingaben zu verzeichnen, denen zugrunde lag, daß unbeteiligte Bürger aufgrund einer Identitätsverwechslung zum Objekt von Vollstreckungsmaßnahmen gemacht wurden. Das grundlegende Problem besteht darin, einen eindeutigen Identifikator (für die übergroße Zahl der Fälle dürfte hierzu neben dem Namen das Geburtsdatum ausreichen) in das Schuldnerverzeichnis zwingend aufzunehmen. Dies ist deshalb schwer zu praktizieren, weil in einem großen Teil der Fälle weder der Gläubiger noch das Gericht das Geburtsdatum kennen: Wenn sich der Schuldner seinen Verpflichtungen dadurch entzieht, daß er in keinem Stadium des Verfahrens persönlich erscheint, läßt sich dieses Geburtsdatum nur schwer feststellen. Dennoch hält der LfD aus folgenden Gründen eine solche Ergänzung der Schuldnerverzeichnisse für erwägenswert:

- Verwechslungsfälle setzen nicht voraus, daß der fälschlich in Anspruch genommene Unbeteiligte auch unter derselben Anschrift wie der Schuldner wohnt. Die Anschrift ist erfahrungsgemäß ein wenig geeignetes Mittel zur Identifizierung, da sie häufigen Änderungen unterliegen kann. Dementsprechend wird in der Praxis auf die Anschrift bei Identitätsfeststellungen nur geringer Wert gelegt. Gerade in kleineren Gemeinden kommt es zudem häufig vor, daß in der gleichen Straße mehrere Personen mit gleichen Vor- und Nachnamen wohnen. Hausnummern treten als Identitätsnachweismerkmal in der Praxis weitgehend in den Hintergrund, da die Erfahrung lehrt, daß hier häufig ungenaue Angaben aufgezeichnet worden sind.

- In den Fällen, in denen eine Verwechslungsgefahr objektiv besteht, ist die Angabe des Geburtsdatums grundsätzlich geeignet, Verwechslungen auszuschließen.

- Grundsätzliche Bedenken gegen die Aufnahme des Geburtsdatums in das Schuldnerverzeichnis dürften von keiner Seite erhoben werden: bereits jetzt wird diese Information in einem relevanten Prozentsatz der Eintragungen gespeichert. Dies erfolgt immer dann, wenn der Schuldner die eidesstattliche Versicherung tatsächlich ablegt. Aus datenschutzrechtlicher Sicht sollte die Feststellung des Schuldnergeburtsdatums möglichst frühzeitig im Vollstreckungsverfahren erfolgen; spätestens aber sollte es möglichst ausnahmslos in das Schuldnerverzeichnis aufgenommen werden, auch wenn sich der Schuldner der Abgabe der eidesstattlichen Versicherung entzieht. Dies sind die Fälle, in denen aufgrund des nicht feststellbaren Wohnsitzes auch die Verwechslungsgefahr besonders groß ist.

- Der entstehende Verwaltungsaufwand wäre bei einer verbindlich vorgeschriebenen Angabe des Schuldnergeburtsdatums durch den Gläubiger als Eintragungsmerkmal im Schuldnerverzeichnis zu vernachlässigen. Der Gläubiger könnte diese Information regelmäßig durch eine Melderegisterauskunft beim Meldeamt erhalten. Die Melderegister werden in Rheinland-Pfalz in automatisierter Form geführt, so daß für die Meldeämter entsprechende Auskunftserteilungen unproblematisch möglich sind.

- Der Aufwand für den Gläubiger selbst wäre ebenfalls gering: Die Angabe des Geburtsdatums gehört zu der Melderegisterauskunft gem. § 34 Abs. 2 MeldeG, die jedem zu erteilen ist, der ein berechtigtes Interesse glaubhaft macht. Bei einer gesetzlichen Regelung, wonach zur Schuldnerbezeichnung im Schuldnerverzeichnis auch Tag und Ort der Geburt gehören, läge nicht nur ein berechtigtes Interesse, sondern ein rechtliches Interesse an dieser Auskunft vor. Im Regelfall könnte der Gläubiger also diese Information leicht und schnell erhalten. In den Fällen, in denen der Schuldner nicht ordnungsgemäß gemeldet ist oder beim Melderegister die Identität des Schuldners nicht zweifelsfrei festgestellt werden kann, wäre im Schuldnerverzeichnis ein entsprechender Vorbehalt bez. der Identität des Schuldners (etwa mit dem Hinweis „im Melderegister nicht ermittelbar") aufzunehmen. Dieser Hinweis würde gleichzeitig eine gewisse Warnfunktion für alle am Vollstreckungsverfahren Beteiligten bezüglich der unsicheren Identitätsfeststellung des Schuldners bewirken.

- Mißbräuchliche Inanspruchnahmen der Melderegisterauskunft, die sich auf das Geburtsdatum bezieht, sind dann nicht zu befürchten, wenn – wovon auszugehen ist – die Meldeämter gesetzeskonform das Vorliegen des berechtigten Interesses nach den dort geltenden allgemeinen Grundsätzen prüfen. Dazu würde beispielsweise gehören, daß grundsätzlich die Gläubigereigenschaft des Anfragenden plausibel dargelegt werden muß.

- Die Verwechslungsgefahren werden künftig erheblich steigen. Die Zentralisierung der Schuldnerverzeichnisse in automatisierten Verfahren ist nicht mehr nur eine abstrakt bestehende Möglichkeit. Private Firmen haben bereits damit begonnen, überregional Schuldnerverzeichnisse automatisiert zu führen (zu nennen ist insbesondere die Firma Infodata GmbH Rastatt im Auftrag der Hans-Soldan-Stiftung). Bei überregionalen Registern steigt erfahrungsgemäß die Verwechslungsgefahr, weil örtliche Kenntnisse und örtliche Bezüge der Sachbearbeiter fehlen. In diesem Zusammenhang kann auf die Erfahrungen des Bundeszentralregisters in Berlin verwiesen werden, das gerade zur Vermeidung von Verwechslungen außerordentliche und begrüßenswerte Anstrengungen unternommen hat. Zumindest im Ansatz sollten die dort vorliegenden Erfahrungen auch im Bereich der Schuldnerverzeichnisse genutzt werden. Dazu gehört die Umsetzung der Erkenntnis, daß die Eingabe des Geburtsdatums als Identifikator unverzichtbar ist.

- Schließlich ist zu berücksichtigen, wie schwer der durch die Verwechslung bewirkte Eingriff in die Rechte des Unbeteiligten wiegt. Hierfür ist auch bedeutsam, welche Schwierigkeiten der fälschlich in Anspruch genommene Bürger hat nachzuweisen, daß er nicht der betroffene Schuldner ist. Diese Schwierigkeiten sind nur dann leicht zu überwinden, wenn das Geburtsdatum des wahren Schuldners feststeht.

Aus datenschutzrechtlicher Sicht dürfte bei einer Abwägung der Nachteile des jetzigen Verfahrens und der Belastungen durch das vom LfD vorgeschlagene Verfahren letzteres den Vorzug verdienen. Der LfD hat gegenüber dem Ministerium der Justiz angeregt, auf geeignetem Weg (wobei auch an administrative Maßnahmen zu denken ist) die Identifikationsmerkmale zu erhöhen. Das Ministerium vertritt derzeit noch die Auffassung, der entstehende Verwaltungsaufwand für die Ermittlung des Schuldnergeburtsdatums durch den Gläubiger stehe in keinem Verhältnis zum möglichen Erfolg. Das (seiner Auffassung nach geringe) Risiko, als Unbeteiligter in ein Vollstreckungsverfahren hineingezogen zu werden, müsse ebenso wie in anderen Lebensbereichen als sozialadäquat hingenommen werden. Aus der Sicht des Datenschutzes kann dies im Interesse des Grundrechts des in ein Vollstreckungsverfahren hineingezogenen Unbeteiligten nicht akzeptiert werden. Der LfD wird seine Bemühungen, Verbesserungen zu erzielen, hier ebenso wie bei vergleichbaren Problemen im Bereich der Melderegister (s. oben Tz. 4.6) fortsetzen.

7.6 Notare

Nach § 10 LDatG hat jede speichernde Stelle die Anwendungen der automatisierten Datenverarbeitungen beim LfD anzumelden. Hierbei sind die in Nrn. 1 – 7 des § 10 Abs. 1 LDatG genannten Angaben zu machen.

Im Bereich der Notare war durch deren Standesvertretungen in Zweifel gezogen worden, ob diese Vorschrift auch für sie gilt oder ob die Bundesnotarordnung nicht für alle Aspekte der Tätigkeit des Notars abschließende Regelungen enthält. Vor dem Hintergrund dieses Streits wurde Anfang 1987 folgende Vereinbarung unter Einbeziehung der Notarkammern und des Justizministeriums getroffen:

Die Notare teilen der jeweiligen Notarkammer mit, welche automatisierten Datenverarbeitungssysteme eingesetzt werden. Die Notarkammern geben über das Justizministerium die entsprechenden Informationen an die DSK weiter. Konkrete Überprüfungsmaßnahmen bezüglich der Einhaltung des Notargeheimnisses sowie der sonstigen Anforderungen des LDatG werden durch die Notardienstaufsicht durchgeführt. Die DSK hat jedoch ausdrücklich betont, daß damit kein Verzicht auf eigene Überprüfungsmaßnahmen gem. § 20 LDatG verbunden sei.

Dieses Verfahren ist grundsätzlich beachtet worden: Die DSK hat eine Reihe von entsprechenden Kurzmitteilungen, ohne die im einzelnen nach § 10 Abs.1 LDatG erforderlichen Angaben, aus dem Notarbereich erhalten. Örtliche Feststellungen hat sie bei den Notaren nicht durchgeführt.

Aufgrund der Entscheidung des BGH vom 30. Juli 1990, in der geklärt wurde, daß eine Anmeldepflicht der Notare nach dem LDatG besteht, hat die DSK mit Schreiben vom 31. Oktober 1990 an das Justizministerium angekündigt, ihre eigenen Befugnisse im Bereich der Notare verstärkt wahrnehmen zu wollen. Zu diesem Zweck hat sie um Mitteilung gebeten, wie und mit welchem Ergebnis die mit der Notardienstaufsicht betrauten Stellen bislang auch Fragen des Datenschutzes überprüft haben. Außerdem hat sie angefragt, ob und ggf. mit welchem Inhalt durch Notare Dienstanweisungen zur Datensicherheit gem. § 9 Abs. 2 LDatG erlassen worden sind.

Aus den übersandten Stellungnahmen der für die Notardienstaufsicht zuständigen Richter ergibt sich, daß spezifisch datenschutzrechtliche Fragen bzw. Fragen des technischen und organisatorischen Datenschutzes bislang bei den Prüfungen nur eine

sehr untergeordnete Rolle gespielt haben. Reaktionen der Notare unmittelbar haben gezeigt, daß diese über ihre gesetzlichen Verpflichtungen häufig nicht informiert sind. Besonders weit verbreitet ist die Auffassung, daß sich besondere Dienstanweisungen zum technischen Datenschutz im Hinblick auf die dem Notar und seinen Mitarbeitern gesetzlich auferlegte umfassende Verschwiegenheitspflicht erübrigen würden. Ein Gespräch mit Notaren hat ergeben, daß dieses Mißverständnis nicht leicht zu beseitigen ist.

Nunmehr hat das Justizministerium angefragt, ob die vereinfachte Form der Anmeldung auch künftig beibehalten werden könnte.

Diese Anregung steht im Gegensatz zur Auffassung des Präsidenten der Notarkammer Pfalz, der mit Schreiben vom 22. Januar 1991 ausgeführt hat:

„Mit Rücksicht auf die von den Software-Herstellern geltend gemachten Urheberrechtsinteressen rege ich an, daß die erforderlichen Anmeldungen künftig unmittelbar gegenüber der Datenschutzkommission gemacht werden."

Aus datenschutzrechtlicher Sicht wäre dies zu befürworten. Der Grund für eine Sonderbehandlung ist entfallen.

8 Kultusbereich

8.1 Wissenschaftliche Forschung

8.1.1 Bereichsspezifische Datenschutzregelungen

Die Tendenz auf der Ebene der Gesetzgebung geht dahin, bereichsspezifische Forschungsklauseln in die Fachgesetze aufzunehmen, um jeweils abhängig vom konkreten Sachzusammenhang die Möglichkeiten von Forschungseinrichtungen zu regeln, personenbezogene Daten von Bürgern zu wissenschaftlichen Zwecken zu nutzen. So ist im Landeskrankenhausgesetz (§ 38) eine entsprechende ausführliche Regelung enthalten; im Landesstatistikgesetz (durch Verweisung auf § 14 Bundesstatistikgesetz) und im Maßregelvollzugsgesetz (durch Verweisung auf § 38 Landeskrankenhausgesetz) bestehen entsprechende Regelungen; es ist geplant, in das Strafvollzugsgesetz und das Gesetz über die psychiatrischen Krankenhäuser (PsychKG) Forschungsregelungen aufzunehmen.

Im Schulgesetz (§ 54 a Abs. 3) besteht bereits seit längerem hierfür eine Sondervorschrift. Das Archivgesetz schließlich hat die wissenschaftliche Nutzung von Archivalien zum zentralen Gegenstand (vgl. hierzu Tz. 8.2).

8.1.2 Epidemiologische Krebsregister

Die Einrichtung sog. epidemiologischer Krebsregister, die Datenerhebung zu diesem Zweck sowie die zulässige Datennutzung sind in Rheinland-Pfalz noch ungeregelt. Dies ist einem Krebsregistergesetz vorbehalten; auf Bundesebene liegt ein erster Entwurf vor. Da auch dieser Entwurf davon ausgeht, daß die eigentliche Registerführung länderbezogen erfolgen soll, sind daneben Überlegungen anzustellen, wie ein derartiges Register in Rheinland-Pfalz geführt werden sollte.

Die Probleme hierbei sind von der DSK in der Vergangenheit wiederholt angesprochen worden. Zu den datenschutzrechtlichen Anforderungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder einen Beschluß gefaßt, der in der Anlage abgedruckt ist (Anlage 2).

Daraus läßt sich ersehen, daß eine gewisse festgefahrene Situation entstanden ist: Aus der Sicht der Datenschutzbeauftragten sind Krebsregister nur zulässig, wenn sie entweder aufgrund der umfassenden Einwilligung der betroffenen Patienten geführt werden oder wenn sie nur anonymisierte Daten enthalten, die allenfalls von der meldenden Stelle (dem behandelnden Arzt) reidentifiziert werden können (sog. dezentrales Verschlüsselungsmodell, in Baden-Württemberg praktisch erprobt). Dies reicht aus der Sicht der betroffenen Wissenschaftler nicht aus.

Zur Zeit werden Überlegungen angestellt, ob ein Kompromiß in diesem Bereich möglich ist. Folgendes Modell wird auf Anregung des Mainzer Instituts für medizinische Statistik und Dokumentation diskutiert:

Die Ärzte sollen das Recht erhalten, Krebserkrankungsfälle an das rheinland-pfälzische Krebsregister zu melden. Soweit ärztlich vertretbar, sollen die Patienten vom meldenden Arzt über die beabsichtigte Datenübermittlung unterrichtet werden. Die erfolgte Unterrichtung ist zu dokumentieren. Widerspricht ein Patient der Meldung, so darf der Arzt nur eine anonyme Meldung weiterleiten. Nur indirekt an der Behandlung beteiligte Stellen, z. B. Pathologen, werden in der Regel die Betroffenen nicht informieren können. Die Meldungen gehen beim Krebsregister in personenbezogener Form ein. Erforderliche Rückfragen sollen kurzfristig bei den meldenden Ärzten abgeklärt werden. Nach Abschluß dieser Rückfragen werden die Datensätze

anonymisiert. Dies soll spätestens nach ca. drei Monaten erfolgen. Der Schlüssel, der es gestattet, Datensätze zu reidentifizieren, soll dem Register nicht zugängig sein, er muß an einer anderen Stelle (einer Treuhandstelle) vorgehalten werden.

Der überwiegende Teil aller wissenschaftlichen Auswertungen soll auf der Basis der anonymisierten Datensätze erfolgen. In Ausnahmefällen wird es zu Situationen kommen, bei denen ein Rückgriff auf personenbezogene Datensätze erforderlich ist, wenn z. B. Zusatzerhebungen bei Ärzten oder Patienten benötigt werden (etwa im Rahmen von Ursachenforschungen). Es ist geplant, unter besonderen Voraussetzungen (z. B. Zustimmung eines wissenschaftlichen Beirats) die jeweils verschlüsselten Identifikationsmerkmale an die Treuhandstelle zu übergeben, die eine Deanonymisierung vornimmt und sie in geeigneter Form an den mit der Durchführung der Forschung betrauten Wissenschaftler weitergibt.

Dieses Modell basiert auf einem Melderecht der behandelnden Ärzte, das nur durch den ausdrücklichen Widerspruch der Betroffenen eingeschränkt wird. Im Register werden grundsätzlich nur anonymisierte Daten gespeichert. Lediglich für eine kurzfristige Bearbeitungsphase, die der Qualitätssicherung der eingehenden Daten dient, bliebe der Personenbezug erhalten, um erforderliche Rückfragen bei den meldenden Ärzten durchführen zu können. Die Anonymisierung würde unter Einsatz eines asymmetrischen Verschlüsselungsverfahrens erfolgen, das eine Deanonymisierung verschlüsselter Datensätze im Krebsregister selbst ausschließt.

Dieser Vorschlag (den man als „Treuhandmodell" bezeichnen könnte) ist – wie sich aus den bislang unter Beteiligung des LfD geführten Gesprächen ergibt – unter Einbeziehung folgender Gesichtspunkte zu bewerten:

a) Im Rahmen der Führung des bundesweiten Kinderkrebsregisters, das auf der Basis der Einverständniserklärung der Eltern in personenbezogener Form geführt wird, wurde die Erfahrung gewonnen, daß in einem relevanten Prozentsatz der Fälle die Meldungen fehlerhaft (unplausibel) sind. Diese Fehler werden bereits bei der Eingabe bemerkt und können im Regelfall durch eine sofortige Rückfrage bei der meldenden Stelle (dem meldenden Arzt) geklärt werden. Dabei ist der Name des betroffenen Patienten nahezu unverzichtbar, um den Aufwand bei der auskunfterteilenden Stelle (dem Arzt) in zumutbaren Grenzen zu halten: Dort muß die Arzthelferin in der Lage sein, ohne erheblichen Aufwand herauszufinden, um welchen Patienten es geht, um dann anhand der dort vorliegenden Patientenunterlagen die offenen Fragen zu klären.

b) Ein weiterer Gesichtspunkt aus der Praxis ist in diesem Zusammenhang bedeutsam:
Nach Angabe von Fachleuten ist es objektiv unvermeidlich, daß – abgesehen von der atypischen Situation des Kinderkrebsregisters – Krebsregister auf der Basis der Einwilligung mit mindestens ca. 30 % nicht gemeldeten Fällen auskommen müssen. Auch wenn diese Fälle darauf beruhen, daß die Ärzte möglicherweise ohne zureichenden Grund davon absehen, sich um die Einwilligung der Patienten zu bemühen, sprechen Experten davon, daß eine solch lückenhafte Erfassung den wissenschaftlichen Wert von Krebsregistern völlig zunichte macht: Dann sei die Verwendung erheblicher Steuermittel auf diesen Bereich nicht vertretbar.

c) Gegen das reine dezentrale Verschlüsselungsmodell, wie es in Baden-Württemberg praktiziert worden sei, sprächen insbesondere folgende Gesichtspunkte:

- Die Klärung von Unplausibilitäten unmittelbar bei der Einspeicherung sei kompliziert.

- Die Möglichkeiten, spätere Fallstudien durchzuführen, seien erschwert: bei der dezentralen Verschlüsselung bestehe die Gefahr, daß die ursprüngliche meldende Stelle (der Arzt, bei dem die Entschlüsselung allein möglich ist) nach längeren Zeiträumen nicht mehr erreichbar ist oder aus sonstigen Gründen eine Entschlüsselung nicht mehr durchführen wolle oder könne.

- Außerdem belaste die dezentrale Verschlüsselung beim Arzt diesen mit weiteren Aufgaben: Es stelle aber grundsätzlich ein großes Problem dar, die Ärzte zur Mitarbeit an einem Meldesystem im Zusammenhang mit Krebsregistern zu motivieren.

Unter Berücksichtigung dieser Überlegungen neigt der LfD dazu, den dargelegten Vorstellungen für eine Kompromißlösung (für ein Melderechtsmodell mit Unterrichtungspflicht durch den Arzt, Widerspruchsrecht des Betroffenen und zentraler Verschlüsselung bei einer Treuhandstelle) näherzutreten. Grundlegend wichtig erscheint dabei, durch eine Bündelung verschiedener Maßnahmen den Eingriff in das informationelle Selbstbestimmungsrecht der Patienten möglichst zu minimieren, so daß es dann bei einer Abwägung zwischen den Forschungsinteressen einerseits und den Individualinteressen andererseits vertretbar wird, daß der Gesetzgeber (dieser muß bei der Einrichtung eines Krebsregisters in jedem Fall tätig werden) gewisse Eingriffe in das informationelle Selbstbestimmungsrecht zuläßt.

Vor einer abschließenden Bewertung aus datenschutzrechtlicher Sicht werden jedoch die hiermit zusammenhängenden Fragen noch im Kreis der Datenschutzbeauftragten erörtert werden.

8.2 Landesarchivgesetz

Bereits 1981 hatte die DSK in ihrem 8. Tätigkeitsbericht auf die Notwendigkeit einer gesetzlichen Regelung des Archivwesens hingewiesen. Nunmehr ist mit Wirkung vom 15. Februar 1991 das Landesarchivgesetz in Kraft getreten.

Dem waren intensive Erörterungen dreier Gesetzentwürfe (eines Regierungsentwurfs sowie je eines Gesetzentwurfs der Fraktionen der SPD und der GRÜNEN) vorangegangen. In diesem Zusammenhang hat die DSK in mündlichen Stellungnahmen vor dem Kulturpolitischen Ausschuß sowie in umfangreichen schriftlichen Stellungnahmen auf aus ihrer Sicht bestehende Defizite und Unklarheiten der Gesetzentwürfe hingewiesen. Sie hat dabei einen deutlichen Schwerpunkt darauf gesetzt, daß ein angemessener Ausgleich zwischen Allgemeininteressen und Individualinteressen erfolgt. Mit anderen Worten: Ziel ihrer Stellungnahmen war nicht, einen absoluten Persönlichkeitsschutz der betroffenen Bürger und Amtsträger zu erreichen, deren Daten in Archivalien gespeichert werden, ihr Ziel war vielmehr, einen Ausgleich zwischen den insbesondere wissenschaftlichen (aber auch sonstigen) Interessen an der Nutzung von Archivalien einerseits und den berechtigten Persönlichkeitsinteressen andererseits herbeizuführen. Der Datenschutz hat in diesem Zusammenhang auch eine besondere Verantwortung gegenüber folgenden Generationen: Archive sollen einen „Informationsvorrat" für noch völlig unvorhersehbare Fragen bereithalten, die in näherer oder fernerer Zukunft an die Vergangenheit gestellt werden. Die DSK hat deshalb Abstand davon genommen, Bestrebungen zu unterstützen, wonach Akten oder sonstige Datenträger zu „anonymisieren" sind, bevor sie an das Archiv weitergeleitet werden. Insbesondere auch die wissenschaftliche Nutzungsmöglichkeit für künftige Forschung wäre damit erheblich gefährdet. Auf ihre Initiative ist eine Regelung zurückzuführen, die es ermöglicht, Unterlagen trotz bestehender Löschungsverpflichtungen dann in das Archiv einzustellen, wenn der durch die Vernichtung oder Löschung bezweckte Schutz der Betroffenen durch eine Aufbewahrung der Unterlagen als Archivgut gewährleistet ist (§ 1 Abs.2 LArchG).

Insgesamt kann gesagt werden, daß das Landesarchivgesetz – trotz einiger gesetzestechnischer Unklarheiten und Mängel, die in erster Linie auf die Übernahme entsprechender Formulierungen des Bundesarchivgesetzes zurückgehen – angemessene Regelungen für diesen Bereich enthält und aus datenschutzrechtlicher Sicht zu begrüßen ist. Zu Fragen der Archivierung im Sozialleistungsbereich s. unten Tz. 11.3.5 .

8.3 Hochschulverwaltung

8.3.1 Datenerhebung und -übermittlung von Studentendaten

Eine Universität des Landes hat angefragt, ob sie an Behörden oder private Dritte Studentendaten übermitteln darf, die zu Verwaltungszwecken anläßlich der Einschreibung erhoben worden sind, oder ob die anfragende Stelle auf den Grundsatz verwiesen werden muß, daß Daten grundsätzlich zunächst beim Betroffenen selbst zu erfragen sind. Zu dieser Grundsatzfrage hat der LfD wie folgt Stellung genommen:

a) Hat eine Datenerhebung beim Betroffenen grundsätzlich Vorrang vor einer Erhebung bei anderen öffentlichen Stellen?

Der Grundsatz der „Erstbefragungspflicht" beim Betroffenen selbst stammt aus dem Abgabenrecht: § 93 Abgabenordnung regelt, daß vor einer Befragung dritter oder anderer Stellen der Betroffene selbst befragt worden sein muß oder daß eine Befragung des Betroffenen selbst erfolglos erscheint. Diese Regelung der AO 1977 ist insoweit im wesentlichen gleichlautend mit einer bereits in der Reichsabgabenordnung (§ 209) enthaltenen Vorschrift.

Der Zweck einer solchen Erstbefragungspflicht ist vielfältig:

- Dritte sollen regelmäßig nicht in das ursprüngliche Verwaltungsverfahren (hier: Besteuerungsverfahren) hineingezogen werden; ihnen sollen die mit der Auskunftserteilung regelmäßig verbundenen Unannehmlichkeiten aller Art solange erspart bleiben, als nicht geklärt ist, ob der Beteiligte selbst den Sachverhalt aufklären kann.

- Die Erstbefragungspflicht dient aber auch dem Interesse des Betroffenen dahin, daß andere Personen über seine Beziehungen zur öffentlichen Hand (hier: Steuerbehörden) nach Möglichkeit nichts erfahren.

- Daneben spielt sicherlich auch eine Rolle, daß Behörden nicht ohne Kenntnis des Betroffenen selbst ihren Informationsstand in bezug auf den Betroffenen erweitern sollen.

Im Regelfall wird es also auch dem informationellen Selbstbestimmungsrecht eher entsprechen, zunächst den Betroffenen zu befragen, bevor Dritte in Anspruch genommen werden.

Der Gesetzgeber ist jedoch nicht von Verfassungs wegen gehindert, hier jeweils bereichsspezifische sachangemessene Lösungen zu treffen, die keine Erstbefragungspflicht beim Betroffenen vorsehen, solange die genannten Gesichtspunkte ausreichend berücksichtigt sind. Auch die neuen Erhebungsregelungen des BDSG (§ 13) stehen dem nicht entgegen. Die in § 13 Abs. 2 BDSG genannten Voraussetzungen lassen im Gegenteil einen sehr weiten Raum für Datenerhebungen bei Dritten. Die Regelungen des BDSG schließlich hindern den Landesgesetzgeber nicht, in Konkretisierung der dort genannten Grundsätze oder auch abweichend davon Regelungen zu treffen.

b) Bezogen auf die Datenübermittlung durch Hochschulen des Landes Rheinland-Pfalz sieht der LfD jedenfalls keine verfassungsrechtlich zwingende Notwendigkeit (eher sogar rechtliche Bedenken), die Einschreibeordnungen um den Grundsatz der Erstbefragungspflicht für Dritte zu ergänzen. Die Formulierung in einigen Einschreibeordnungen über Datenübermittlungen an Dritte ist zwar nicht so klar und am Zweckbindungs- wie am Verhältnismäßigkeitsgrundsatz orientiert, wie dies wünschenswert wäre. Nach dem Wortlaut der Satzungsermächtigung in § 63 Abs. 3 Nr. 2 HochschG wäre eine Konkretisierung der Übermittlungsregelungen in den Einschreibeordnungen einiger Hochschulen sicherlich, wenn nicht erforderlich, so doch zumindest wünschenswert. Vorbildlich ist insoweit die entsprechende Regelung der Einschreibeordnung der Hochschule für Verwaltungswissenschaften Speyer, die als Beispiel einer genügend konkreten Regelung herangezogen werden kann. Fraglich ist allerdings, ob die einzelne Hochschule Erstbefragungspflichten der anfragenden Dritten per Satzung normieren kann, da die Satzungsbefugnis der Universitäten wohl nicht soweit geht, Handlungspflichten Dritter zu begründen. Das BDSG ermöglicht der übermittelnden Stelle grundsätzlich nicht, die Einhaltung der Erstbefragungspflicht durch die anfordernde Stelle zu überprüfen (§ 15 Abs.2 Satz 2 BDSG ; anders allerdings, wenn private Dritte Empfänger sind, § 16 Abs.2 BDSG).

c) Aus der Zulässigkeit einer Datenübermittlung an Dritte folgt nur dann die Pflicht zur Übermittlung der Daten, wenn eine entsprechende Rechtsvorschrift dies bestimmt. In Betracht käme § 4 Abs. 1 Verwaltungsverfahrensgesetz des Bundes (anzuwenden gem. § 1 Landesverwaltungsverfahrensgesetz). Die in §§ 5, 6, 7 und 8 VwVfG geregelten Ausnahmen und Bedingungen, unter denen Amtshilfe zu leisten ist, schränken auch diese Pflicht zur Amtshilfe ein. Gemäß § 5 Abs. 1 Nr. 2 VwVfG ist auch der faktische Aufwand, der zu Erfüllung der Amtshilfepflicht erforderlich ist, bedeutsam.

Festzuhalten bleibt, daß allein aufgrund der Amtshilfevorschriften keine Befugnis zur Datenübermittlung besteht. Wenn jedoch aus anderen Regelungen eine Datenübermittlungsbefugnis herzuleiten ist, ist die Frage, ob eine Pflicht der ersuchten Behörde zur Übermittlung der Daten besteht, nach den Regelungen über die Amtshilfe (§§ 4 ff. VwVfG) zu beantworten.

Falls der Datenempfänger eine private Stelle ist, haben im Rahmen des dann auszuübenden Ermessens die Gesichtspunkte des Verwaltungsaufwands besondere Bedeutung.

Über seine Rechtsauffassung hat der LfD sowohl die anfragende Universität wie das zuständige Ministerium informiert.

8.3.2 Pauschale Unterrichtung der Schulaufsichtsbehörden aller Bundesländer über das Nichtbestehen der Feststellungsprüfung im Ausländerzulassungsverfahren an Hochschulen

Die Kultusministerkonferenz hat mit Beschluß vom 30. April 1976 in der Fassung vom 18. September 1987 eine Rahmenordnung der Prüfung zur Feststellung der Eignung ausländischer Studienbewerber für die Aufnahme eines Studiums an Hochschulen der Bundesrepublik Deutschland beschlossen.

In Ziffer 9 dieser Ordnung ist geregelt, daß die Prüfung nur einmal vor dem Prüfungsausschuß des gleichen Studienkollegs wiederholt werden kann. In Nr. 10 der Ordnung ist bestimmt, daß dann, wenn der ausländische Studienbewerber die Feststellungsprüfung nicht bestanden hat, die für die Prüfung zuständige Abteilung des Kultusministers unverzüglich die Schulaufsichtsbehörden aller anderen Länder zu unterrichten hat.

Hierauf hat der Berliner Datenschutzbeauftragte aufmerksam gemacht. Datenschutzrechtlich ist dieses Verfahren unzulässig.

a) Die Datenerhebung durch Nutzung übersandter Informationen verstößt gegen den Grundsatz, daß Daten bei anderen öffentlichen Stellen ohne Kenntnis des Betroffenen nur in eng begrenzten Ausnahmefällen erhoben werden dürfen (vgl. jetzt auch § 14 BDSG).

b) Auch die Übermittlung solcher Informationen an andere Kultusbehörden verstößt gegen Datenschutzrecht (§ 6 Abs. 1 LDatG), da danach nur solche Datenübermittlungen erlaubt sind, die zur rechtmäßigen Erfüllung der durch Gesetz der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgaben erforderlich sind. Diese Erforderlichkeit ist jedoch nicht gegeben und kann auch nicht damit begründet werden, daß allen ausländischen Studienbewerbern, die die Feststellungsprüfung nicht bestanden haben, unterstellt wird, sie würden durch Tauschung die Zulassung zu weiteren Feststellungsprüfungen an anderen Hochschulen anstreben.

Vergleichbare Problemfälle haben sich in der Vergangenheit bei einer Vielzahl sog. „Warndateien" ergeben. Hier wurde auch von der DSK regelmäßig die Erforderlichkeit einer Datenübermittlung in Abrede gestellt, die an alle in Betracht kommenden Stellen flächendeckend erfolgt. In Fortsetzung dieser Beurteilung ist der LfD der Auffassung, daß auch im vorliegenden Fall ein flächendeckender Informationsaustausch nicht erforderlich ist. Andererseits ist nicht zu bestreiten, daß eine wirksame Kontrolle ohne die Möglichkeit einer zentralen Abfrage kaum vorstellbar ist. Es wäre zu überlegen, ob es dem Verhältnismäßigkeitsgrundsatz entsprechen würde, eine Zentralstelle zu bestimmen, bei der jeweils nur abgefragt wird, ob ein bestimmter Bewerber im Verzeichnis der erfolglosen Bewerber enthalten ist. Die Einrichtung einer solchen Zentralstelle bedürfte einer gesetzlichen Grundlage.

Über diese Rechtsauffassung wurde das zuständige Ministerium informiert. Die Erörterungen sind noch nicht abgeschlossen.

9 Umweltschutz

9.1 Altlastenkataster

9.1.1 Allgemeines

Die Grundlage wirksamer Umweltschutzmaßnahmen sind Informationen über die Umwelt und die schädigenden Einflüsse auf die Umwelt. Dementsprechend werden immer häufiger und in immer größerem Umfange Informationen über Art und Ausmaß von Umwelteinwirkungen sowie über Gesundheits- und Umweltgefährdungen systematisch gesammelt und in Dateien, besonderen Verzeichnissen, Katastern oder Kartierungen nachgewiesen. Der Umfang derartiger Datensammlungen und die Anforderungen an die Verfügbarkeit der Daten zwingen zum Einsatz der automatisierten Datenverarbeitung.

Einen Schwerpunkt stellen – auch aus datenschutzrechtlicher Sicht – sogenannte Altlasten –, Altstandort- und Altablagerungskataster dar. Datenschutzrelevant sind derartige Kataster insbesondere deshalb, weil sie grundstücksbezogen, und damit auch personen- oder betriebsbezogen, Informationen nachweisen, die von hoher Empfindlichkeit sind. Das Vorhandensein von Altlasten oder auch nur der Verdacht mindern den Grundstückswert; bisweilen können aus Hinweisen auf Altlasten Folgerungen bezüglich bestehender, die Existenz eines Betriebes gefährdender Sanierungsverpflichtungen gezogen werden.

In Rheinland-Pfalz sind in den letzten Jahren die Altablagerungen von Grundstücken systematisch erfaßt worden. In einem nächsten Schritt soll mit der Erforschung kontaminierter Altstandorte begonnen werden. Die Dokumentation der Ergebnisse dieser Maßnahmen und die Schaffung eines Informationspools zielen auf die Einleitung von Sanierungsmaßnahmen unter Berücksichtigung des jeweiligen Gefährdungspotentials.

Das Zusammenwirken vieler Behörden bei der Einleitung und Durchführung derartiger Maßnahmen wie auch die Anforderungen des Grundstücksverkehrs führen zu der Frage, wie Auskünfte aus den genannten Katastern in datenschutzrechtlicher Hinsicht zu beurteilen sind. Ein besonderes Problem besteht darin, daß es sich häufig um altlastenverdächtige Flächen handelt, über die Daten aufgrund pauschaler Erhebungen gewonnen wurden.

9.1.2 Regelungsbedarf

In ihrem 12. Tätigkeitsbericht beurteilte die DSK unter Tz. 8.4 die Datenverarbeitungsproblematik vor dem Hintergrund des geltenden LDatG. Sie wies darauf hin, daß diesem Gesetz Lösungssätze nur für einen Teil der in den Katastern gespeicherten Daten, nämlich die personenbezogenen Daten entnommen werden konnten. Hinsichtlich solcher Daten hatten die Betroffenen grundsätzlich Auskunftsanspruch, der sich auch auf nicht verifizierte Daten, die gegenüber Dritten nach allgemeinem Datenschutzrecht zu sperren sind, bezog. Die Übermittlung personenbezogener Katasterdaten war ohne Zustimmung der betroffenen Grundstückseigentümer nur dann zulässig, wenn es sich um gesicherte Informationen handelte und Übermittlungsempfänger eine Behörde oder sonstige öffentliche Stelle war, die diese Informationen zur rechtmäßigen Aufgabenerfüllung benötigte. In allen Fällen bestand ein Zustimmungsvorbehalt. Die auf der Grundlage des bestehenden Datenschutzrechts und des Verwaltungsverfahrensgesetzes gefundenen Lösungen waren unter mehreren Gesichtspunkten unbefriedigend. Die einseitige Privilegierung von Datenübermittlungen zwischen Behörden führt zu einer unangemessenen Ausgrenzung öffentlicher und privater Interessen bei umweltrelevanten Informationen. Dies kann sich leicht als akute Gefahr für einen wirksamen Umweltschutz erweisen: Je mehr gravierende Umweltschutzverletzungen bekannt werden, desto deutlicher wird nämlich, daß ohne die Wachsamkeit der örtlichen Bewohner, ohne ihre besondere Kenntnis der Verhältnisse des Einzelfalles, ohne die kritische Mitwirkung fachkundiger Bürger und von diesen befragten Experten viele dieser Fälle noch unbekannt wären und ihre gefährlichen Auswirkungen weiter im Dunkel der Geheimhaltung durch Wirtschaftsunternehmen und/ oder Behörden die Anwohner beeinträchtigen würden (vgl. Schindel in Datenschutz contra Umweltschutz ZRP 1990, S. 135)

Außerdem fehlt es an normenklaren gesetzlichen Regelungen für die Datenerhebung und Datenverarbeitung. Generalklauseln wie sie das LDatG enthält, sind vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts kaum noch geeignet, Informationseingriffe zu legitimieren.

Daß eine auf Herstellung der gebotenen Transparenz zielende Rechtsentwicklung durchaus nicht im Widerspruch zu grundgesetzlich verbürgten Rechtspositionen steht, wird vom Bundesverfassungsgericht in seinem Volkszählungsurteil anerkannt: Im Hinblick auf die Gemeinschaftsgebundenheit und Gemeinschaftsbezogenheit der Person ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet (BVerfGE 65, 1).

9.1.3 EG-Richtlinie über den freien Informationszugang

Konkret vorgezeichnet wird die Weiterentwicklung des Datenschutzrechts im Umweltbereich durch das Recht der Europäischen Gemeinschaften. Nach Art. 3 Abs. 1 Satz 1 der Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (ABL. 158 vom 23. Juli 1990) gewährleisten die Mitgliedstaaten grundsätzlich, daß die Behörden verpflichtet werden, allen natürlichen oder juristischen Personen auf Antrag ohne Nachweis eines Interesses Informationen über die Umwelt zur Verfügung zu stellen. Die Ausnahmeregelung des Artikel 3 Absatz 2 läßt zwar zu, den Zugang zu derartigen Informationen abzulehnen, wenn u. a. Geschäfts- und Betriebsgeheimnisse sowie die Vertraulichkeit personenbezogener Daten und/ oder Akten berührt werden. Dennoch wird der Grundsatz der Informationsfreiheit deutlich akzentuiert; die Offenbarung umweltbezogener Daten soll im Regelfall möglich sein.

An dieser Zielvorgabe – die bis zum 31. Dezember 1992 umzusetzen ist – muß sich der Gesetzgeber bei der Weiterentwicklung des Abfallrechts und speziell bei der Schaffung bereichsspezifischer Vorschriften über Altlastenkataster orientieren.

9.1.4 Novellierung des Landesabfallgesetzes

In Rheinland-Pfalz ist dies durch die Novellierung des Landesabfallgesetzes in einem wichtigen Teilbereich geschehen. Dabei bestimmten umweltpolitische Akzente und die erwähnten rechtlichen Vorgaben gleichermaßen die Zielrichtung: Für Altlasten wurde ein gestuftes und verfahrensmäßig im Detail bestimmtes Ermittlungs- und Nachweissystem eingeführt. Dieser Abstufung entsprechen Informationsregelungen, die das Prinzip der Geheimhaltung für nicht gesicherte Erkenntnisse über Altlasten aufrecht erhalten, den Zugang zu gesicherten Informationen aber deutlich erleichtern.

Solange eine Gefahrenbeurteilung nicht durchgeführt ist, werden Daten in einem Altablagerungs- und Altstandortkataster gespeichert. Aus diesem Kataster dürfen sie nur an die Bezirksregierungen sowie auf Verlangen an die Träger der Bauleitplanung und an die Baugenehmigungsbehörden übermittelt werden, soweit dies zur Erfüllung der diesen Behörden obliegenden Aufgaben erforderlich ist. Nach einer Erfassungsbewertung werden altlastverdächtige und als Altlast eingestufte Flächen beim Landesamt für Umweltschutz und Gewerbeaufsicht in einem zentralen Verdachtsflächen- und Altlastenkataster auf der Grundlage des Liegenschaftskatasters nachgewiesen. § 27 Abs. 7 des Landesabfallwirtschafts- und Altlastengesetzes (Bezeichnung nach Neufassung) läßt die Übermittlung des Inhalts der Verdachtsflächen- und Altlastenkatasters an andere Behörden und Einrichtungen des Landes, der Gemeinden, der Landkreise und kreisfreien Städte zur Wahrung der diesen Stellen auf dem Gebiet der Gefahrenermittlung, Gefahrenabwehr, Überwachung oder Planung gesetzlich obliegenden Aufgaben zu. Die Offenbarungsbestimmungen werden flankiert durch besondere Pflichten zur Benachrichtigung der Betroffenen und Befugnisse zur Unterrichtung der Öffentlichkeit.

Der Gesetzgeber hat in diesem Teilbereich den Gegensatz zwischen den Geheimhaltungsinteressen einzelner und der Notwendigkeit, Umweltschäden aufzuklären, sie zu beseitigen und der Bevölkerung durch eine hinreichend offene Informationspolitik die Teilnahme an der demokratischen Willensbildung und Kontrolle zu ermöglichen, in praktischer Konkordanz gelöst.

9.2 Landeswassergesetz

In ihrer Stellungnahme zu Fragen des Umweltschutzes im 12. Tätigkeitsbericht wies die DSK unter Tz. 8 auf Probleme hin, die zu einem erheblichen Teil auf dem Fehlen normenklarer gesetzlicher Regelungen für die Datenerhebung und Datenverarbeitung beruhen. Generalklauseln, wie sie das LDatG enthält, sind vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts kaum noch geeignet, Informationseingriffe zu legitimieren. Die DSK unterstrich die Forderung nach Schaffung gesetzlicher Regelungen für Informationseingriffe durch Hinweise auf Datenverarbeitungsverfahren im Geschäftsbereich des Ministeriums für Umwelt und Gesundheit – Wasserwirtschaftliches Informationssystem, automatisierte Trinkwasserdatenbank und, besonders detailliert, Einrichtung eines Landesabwasserkatasters –.

Gleichwohl enthielt der von der Landesregierung eingebrachte Entwurf eines Änderungsgesetzes zum Landeswassergesetz mit Ausnahme einer Verweisung allgemeiner Art keine gesetzlichen Regelungen über die Datenerhebung, die Datenverarbeitung und den Datenschutz. Der Referentenentwurf war der DSK nicht zur Stellungnahme vorgelegt worden.

Die Empfehlung der DSK, den Entwurf um Regelungen der vorbezeichneten Art zu ergänzen, wurde erst in der parlamentarischen Beratung aufgegriffen. Das vom Landtag verabschiedete Gesetz nennt in § 109 a die zulässigen Datenerhebungs- und ver-

arbeitungszwecke und bestimmt, an welche Maßnahmenträger Daten zur Aufgabenerfüllung weitergegeben werden dürfen. § 127 gestattet die Einsicht in das Wasserbuch für jedermann (Landeswassergesetz vom 14. Dezember 1990, GVBl. 1991 S. 11, BS 75-50).

10 Gesundheitswesen

10.1 Weitergabe von Daten aus amtsärztlicher Untersuchungstätigkeit

Aufgrund einer Anregung der DSK erließ das Ministerium für Umwelt und Gesundheit 1986 eine Verwaltungsvorschrift, die auf die Einschränkung der Weitergabe von Daten aus amtsärztlicher Untersuchungstätigkeit in dienst- und arbeitsrechtlichen Angelegenheiten zielt (MinBl. 1986, S. 146). Konkret ist in dieser Verwaltungsvorschrift bestimmt, daß die Gesundheitsämter den anfordernden Stellen „das Untersuchungsergebnis" unter Verwendung eines Formblattes mitteilen und daß solche Daten, die die Beurteilungsgrundlage bilden, bei den Gesundheitsämtern verbleiben.

Die DSK erhielt wiederholt Eingaben, die die Weitergabe von Untersuchungsdaten und anderen Informationen durch Gesundheitsämter an Dienstbehörden betrafen. Ein besonders drastischer Fall, der auch beträchtliches öffentliches Aufsehen erregte, war auch im Berichtszeitraum zu bearbeiten:

Ein Gesundheitsamt war unter Mitteilung der Vorerkrankungszeiten einer Bediensteten – elf Wochen innerhalb des vorangegangenen Jahres – gebeten worden, zu der Frage Stellung zu nehmen, ob und ggf. wann die Wiederherstellung der Arbeitsfähigkeit zu erwarten sei. Außerdem wurde eine gutachtliche Äußerung erbeten, ob auch in Zukunft mit häufigen und langandauernden krankheitsbedingten Abwesenheiten vom Dienst gerechnet werden müsse.

Der Amtsarzt ermittelte zunächst durch Befragung der Betroffenen die Ursachen für das wiederholte Fernbleiben vom Dienst und teilte diese der Dienstbehörde mit. Für die Mitteilung seiner Untersuchungsergebnisse verwendete er nicht den vorgeschriebenen Vordruck, sondern berichtete in Briefform. Im übrigen äußerte er Vermutungen, die sich auf den Arbeitswillen bezogen, und beschrieb das Verhalten der Betroffenen während der Untersuchung.

Selbstverständlich war die Betroffene über diesen Inhalt des Briefes, nachdem er ihr vom Arbeitgeber eröffnet worden war, verärgert; sie beschwerte sich bei der DSK.

Auf die Befugnis für die Offenbarung besonders geschützter Daten (§ 2 der Berufsordnung für die Ärzte, § 203 Abs. 1 StGB) angesprochen vertrat der Amtsarzt die Auffassung, daß nicht das übliche Arzt-Patientenverhältnis bestehe. Vielmehr handele das Gesundheitsamt im Auftrag einer anderen Behörde, der es auskunftspflichtig sei. Im übrigen unterscheide sich das Schreiben an die Dienstbehörde in Form und Inhalt „in nichts von gleich oder ähnlich gelagerten Aufträgen, bei denen in aller Regel nie Schweigepflichtsentbindungen des zu Untersuchenden gegenüber dem Arbeitgeber vorliegen". Der Betroffenen seien die Gründe der Einbestellung und der Zweck der Untersuchung erläutert worden.

Das Ministerium meinte, daß der Amtsarzt von der konkludenten Einwilligung in die Offenbarung der Ursachen für Vorerkrankungen ausgehen konnte, weil die Betroffene ein positives – sie vom Verdacht der Drückebergerei entlastendes – Interesse daran haben sollte, daß der Krankheitsgrund transparent gemacht werde. Im übrigen wurde argumentiert, daß nach § 203 Abs. 1 StGB nur die Offenbarung von „Tatsachen" strafbedroht sei. Bei den Äußerungen des Amtsarztes handele es sich um subjektive Wertungen, die nicht § 203 Abs. 1 StGB unterfielen. Immerhin räumte das Ministerium ein, daß solche Wertungen nicht zum Gegenstand einer amtsärztlichen Beurteilung gemacht und vor allem nicht der Dienstbehörde mitgeteilt werden sollten, weil sie geeignet seien, das Ansehen der Person zu schädigen.

Die DSK kam zu dem Ergebnis, daß gegen gesetzliche Bestimmungen verstoßen wurde und begründete dies wie folgt:

Die kraft autonomen Satzungsrechts der Landesärztekammer gem. § 14 Abs. 1 des Heilberufsgesetzes ergangene Berufsordnung für die Ärzte trifft in § 2 Abs. 1 eine inhaltliche Bestimmung der Schweigepflicht, die umfassender ist als die Strafbewehrung in § 203 StGB. Der Schweigepflicht nach § 2 der Berufsordnung unterliegen nicht nur Tatsachen aus dem ärztlichen Berufsbereich, sondern jedwede Wahrnehmung des Arztes oder Mitteilungen, die dem Arzt zugegangen sind. Eine Offenbarungsbefugnis hätte nach § 2 Abs. 5 der Berufsordnung nur dann bestanden, wenn der Betroffenen vor der Untersuchung bekannt gewesen oder eröffnet worden wäre, inwieweit die Feststellungen des Arztes zur Mitteilung an Dritte bestimmt sind. Die erwähnten Satzungsbestimmungen stellen für die Angehörigen des ärztlichen Berufsstandes rechtsverbindliche Normen dar, deren Anwendung der standesrechtlichen und – im öffentlichen Bereich – der dienstrechtlichen Kontrolle unterliegt.

Die der Betroffenen erläuterten Untersuchungsgründe und -zwecke konnten sich nur aus den Fragen der Beschäftigungsbehörde,

- wann mit der Wiederherstellung der Arbeitsfähigkeit zu rechnen sei und

- ob in Zukunft mit häufigen und längere Zeit andauernden Fehlzeiten zu rechnen sei, ergeben. Eröffnet und damit bekannt war der Betroffenen also nur, daß konkrete Fragen beantwortet werden sollten. Sie konnte davon ausgehen, daß dies in knapper Form geschieht.

Danach waren nach Auffassung der DSK Bestimmungen der Berufsordnung für Ärzte insoweit verletzt, als der Amtsarzt der Dienstbehörde ohne ausdrückliche Zustimmung der Betroffenen Diagnosen oder Ursachen für früheres Fernbleiben vom Dienst und seine Bewertung des Verhaltens der Betroffenen bei der Untersuchung mitteilte. Als weiteren Verstoß gegen datenschutzrechtliche Vorschriften wertete sie die Nichtbeachtung der Verwaltungsvorschrift über das verkürzte amtsärztliche Zeugnis.

Der Vorgang ist in diesem Tätigkeitsbericht deshalb in aller Ausführlichkeit dargestellt, weil er geradezu als Lehrbeispiel für die Unsicherheit der Gesundheitsämter bei der Anwendung standesrechtlicher und strafrechtlicher Geheimhaltungsbestimmungen dienen kann. Dabei ist die Rechtslage verhältnismäßig einfach: Wenn – wie im öffentlichen Dienstrecht – keine Offenbarungsbefugnis nach Gesetz oder Tarifvertrag besteht und andere Rechtfertigungsgründe – z. B. rechtfertigender Notstand – nicht in Betracht kommen, benötigt der Arzt zur Offenbarung der Informationen, die er bei der Untersuchung gewinnt, die Einwilligung des Betroffenen. Kommt der Betroffene der Aufforderung, sich untersuchen zu lassen, nach, so kann der Arzt von der konkludenten Einwilligung in die Weitergabe des „Untersuchungsergebnisses" an die Stelle ausgehen, die eine Untersuchung aufgrund gesetzlicher Vorschriften veranlaßt hat. Für jede weitergehende Information benötigt er die ausdrückliche Einwilligung. Es ist stets zu beachten, daß ein öffentlich Bediensteter durchaus ein schutzwürdiges Interesse daran haben kann, daß die Ergebnisse einer ärztlichen Untersuchung, der er sich im Rahmen seines Dienstverhältnisses unterzieht, nicht in seine Personalakten eingehen. Er nimmt, wenn er die Zweifel, die Veranlassung für die Untersuchung waren, nicht ausräumt, zwar in Kauf, dienstrechtliche oder dienstordnungsrechtliche Nachteile zu erfahren. Die Dienstbehörde kann in diesem Falle nämlich auch ohne Vorliegen des ärztlichen Untersuchungsberichtes zu seinem Nachteil entscheiden. Diese Entscheidung kann im Einzelfall für den Betroffenen aber weniger schwerwiegend sein als eine negative Beurteilung seines Gesundheitszustands, die auf Dauer seine Personalakten belastet.

Angesichts der verbreiteten Unsicherheit der Bediensteten von Gesundheitsämtern über die gesetzlichen Grundlagen der Verschwiegenheitspflichten und den Umfang von Offenbarungsbefugnissen empfahl die DSK dem zuständigen Ministerium, die Rechtslage in einem Rundschreiben zu erläutern. Da dies aus der Sicht des Ministeriums in angemessener Zeit nicht zu realisieren war, gab die DSK in der Schriftenreihe „Informationen zum Datenschutz" ein Heft mit dem Titel „Datenschutz im öffentlichen Gesundheitsdienst" heraus. In diesem Heft sind die wichtigsten rechtlichen Bestimmungen kommentiert und für die praktische Arbeit nützliche Materialien – Gesetze, Auszüge aus Stellungnahmen und aus Tätigkeitsberichten der DSK – abgedruckt. Durch Teilnahme an Dienstbesprechungen der Amtsärzte und anderen Veranstaltungen leisteten Mitarbeiter der Behörde des LfD praktische Aufklärungsarbeit.

Anzumerken ist noch, daß die Datenschutzbeauftragten eine gesetzgeberische Initiative anstreben, die darauf gerichtet ist, die Einwilligung als Rechtfertigung einer Offenbarung medizinischer Informationen an die Dienstbehörde durch eine bereichsspezifische gesetzliche Regelung zu ersetzen. Durch eine streng am Erforderlichkeitsgrundsatz orientierte Offenbarungsbefugnis der Amtsärzte soll das Problem gelöst werden, daß eine Einwilligung faktisch erzwungen wird, wenn z. B. eine umfassende Überprüfung zwar als von der Einwilligung des Betroffenen abhängig erklärt wird, seine Bewerbung jedoch nicht berücksichtigt wird oder seine weitere Verwendung auf einem Dienstposten ausscheidet, wenn er die Einwilligung verweigert. Immer dann, wenn bestimmte Angaben verfügbar sein müssen, sollen sie daher präzise gesetzlich vorgeschrieben, zugleich aber auch auf den erforderlichen Umfang begrenzt sein (vgl. die als Anlage 1 abgedruckte Entschließung der DSB-Konferenz).

10.2 Landesgesetz über psychiatrische Hilfen und Schutzmaßnahmen

Das geltende Unterbringungsgesetz vom 19. Februar 1959 ist dringend novellierungsbedürftig. Es wird dem heutigen Verständnis und den Möglichkeiten der modernen Psychiatrie nicht mehr gerecht. Aus der Sicht des Datenschutzes ist zu beklagen, daß es keine speziellen Regelungen über Informationseingriffe, die in diesem Bereich besonderes Gewicht haben, enthält.

Das Ministerium für Soziales, Familie und Sport plante eine umfassende Neugestaltung des Unterbringungsrechts. Gegen Ende der 12. Wahlperiode legte es den Referentenentwurf eines Landesgesetzes über psychiatrische Hilfen und Schutzmaßnahmen (PsychHG) zur Stellungnahme vor. In die Entwurfsfassung wurden auch Bestimmungen über Unterrichtungs- und Akteneinsichtsrechte der Betroffenen und über den Datenschutz aufgenommen. Eine Lösung wurde im wesentlichen dadurch angestrebt, daß die Datenschutzregelungen des Landeskrankenhausgesetzes (§§ 36 und 37 LKG) übernommen werden sollten.

Die DSK hielt demgegenüber eine Differenzierung für geboten. Sie unterstützte den Lösungsansatz für den Bereich der Unterbringungseinrichtungen (psychiatrische Krankenhäuser, psychiatrische Fachabteilungen sonstiger Krankenhäuser, Einrichtungen der Suchtkrankenhilfe, Pflegeheime für psychisch Behinderte und ähnliche anerkannte Einrichtungen), hielt die Vorschriften aber für wenig geeignet, die speziellen Datenschutzprobleme in den Sozialpsychiatrischen Diensten zu lösen, denen die ambulante ärztliche und psychosoziale Beratung und Betreuung obliegt.

Auch die neue Landesregierung hält die Novellierung des Unterbringungsgesetzes für dringlich. Eine Erörterung von Lösungsmöglichkeiten mit Vertretern des Ministeriums für Arbeit, Soziales, Familie und Gesundheit läßt erwarten, daß dem Landtag ein Entwurf zur Beratung und Beschlußfassung vorgelegt wird, der ausgewogene Datenschutzregelungen enthält.

10.3 Sozialpsychiatrische Dienste der Gesundheitsämter

Unter Tz. 9.2.2 ihres 12. Tätigkeitsberichts schilderte die DSK die Probleme, mit denen sich die in den Sozialpsychiatrischen Diensten der Gesundheitsämter tätigen Sozialarbeiter konfrontiert sehen. Einerseits unterliegen sie als Angehörige einer in § 203 StGB genannten Berufsgruppe besonderen strafbewehrten Verschwiegenheitspflichten, andererseits wird von Vorgesetzten im Rahmen der Weisungs- und Kontrollbefugnisse in aller Regel der Anspruch auf vollständige Information über die Tätigkeit, insbesondere auch über den Inhalt von Beratungsgesprächen, erhoben.

Die DSK hatte in ihrem Berichtsbeitrag zwar betont, daß der Regelungsbedarf wohl nur vom Gesetzgeber zu befriedigen sei, dennoch begrüßte sie es, daß das Ministerium für Umwelt und Gesundheit einen Richtlinienentwurf vorlegte, der datenschutzrechtlich vertretbare Lösungsansätze enthielt.

Hervorzuheben ist insbesondere, daß die Betroffenen über die notwendigen Offenbarungen im innerdienstlichen Bereich informiert und so in die Lage versetzt werden sollten, ihr informationelles Selbstbestimmungsrecht auszuüben. Die DSK unterbreitete eine Reihe von Verbesserungsvorschlägen, die von dem zuständigen Ressort auch weitgehend akzeptiert wurden.

Die Hoffnung auf baldige Veröffentlichung der Richtlinien erfüllte sich indessen nicht. Es ist davon auszugehen, daß diese im Blick auf das in Vorbereitung befindliche Landesgesetz über psychiatrische Hilfen und Schutzmaßnahmen (vgl. Tz. 10.2) unterblieben ist. Dennoch kann davon ausgegangen werden, daß auch in der Übergangszeit noch Klarstellungen im Sinne der Richtlinien sinnvoll gewesen wären.

10.4 Schulgesundheitspflege

Die Erfassung und Verarbeitung von medizinischen Daten aus den Schulgesundheitsuntersuchungen auf transportablen PC, sog. Laptops, stellt besondere Anforderungen an die Qualität des technischen und organisatorischen Datenschutzes. Der 12. Tätigkeitsbericht der DSK enthielt unter Tz. 9.4 die Beschreibung eines rheinland-pfälzischen Pilotprojekts sowie des Forderungskatalogs bezüglich der Datensicherung.

Die örtliche Überprüfung eines der Pilotprojekte im Februar 1990 ergab, daß die bereits im März 1989 geforderte Implementierung einer speziellen Sicherungssoftware noch nicht realisiert war. Auch eine Dienstanweisung über die technischen und organisatorischen Datenschutzmaßnahmen, wie sie § 9 LDatG fordert, existierte zu diesem Zeitpunkt noch nicht.

Im Mittelpunkt der vor der Verfahrenseinführung erörterten Maßnahmen zur Verbesserung des technischen und organisatorischen Datenschutzes stand die Verschlüsselung der Daten auf den Festplatten der Laptops. Durch diese Verschlüsselung sollte gewährleistet werden, daß Daten, außer in den Laptops, nur in solchen Geräten weiterverarbeitet werden können, die über eine geeignete und zugelassene Entschlüsselungssoftware verfügen. Die Sicherungsmaßnahmen sollten insbesondere darauf gerichtet sein, die Anfertigung von lesbaren Kopien auf Datenträgern zu verhindern.

Die Überprüfung eines anderen Pilotprojekts im August 1991 ergab, daß die Daten noch immer unverschlüsselt gespeichert sind, damit auch kopiert und in jedem unter MS-DOS betriebenen PC weiterverarbeitet werden können.

Gegenüber dem Ministerium für Arbeit, Soziales, Familie und Gesundheit stellte der LfD fest, daß die Maßnahmen zur Gewährleistung des technischen und organisatorischen Datenschutzes nicht angemessen im Sinne des § 9 LDatG sind und forderte unter Fristsetzung eine entsprechende Verfahrensänderung.

Zu dem Verfahren war ferner folgendes anzumerken:

Die Erforderlichkeit der Einführung eines automatisierten Verfahrens im Jugendärztlichen Dienst wurde ursprünglich damit begründet, daß nur eine umfassende Dokumentation in Verbindung mit qualifizierten Auswertungsverfahren die Möglichkeit biete, einen allgemeinen Überblick über den Gesundheitszustand von Kindern und Jugendlichen und Erkenntnisse darüber zu

gewinnen, wodurch Gesundheitsgefährdungen entstehen und in welcher Weise ihnen durch den öffentlichen Gesundheitsdienst wirksam begegnet werden kann. Es war beabsichtigt, die dokumentierten Untersuchungsbefunde unter Anwendung von Verfahren und Instrumenten der Medizinischen Statistik auszuwerten. Diese wichtigen gesundheitspolitischen Zielsetzungen wurden bei Besprechungen mit Vertretern der DSK immer wieder hervorgehoben.

Bei dem zuletzt geprüften Gesundheitsamt war indessen zu erfahren, daß bisher nichts getan wurde, um diesen eigentlichen Projektzielen näherzukommen. Es existierten keine Auswertungsprogramme, und es war unklar, ob solche in der Zukunft erstellt werden. Zur Zeit werden mit erheblichem technischem Aufwand – und erheblichen Kosten – unter Hinnahme eines beträchtlichen Datenschutzrisikos große Datenmengen erfaßt und ausgedruckt. Der LfD empfahl dem Ministerium zu prüfen, ob eine Übernahme des Verfahrens durch andere Gesundheitsämter auch dann in Betracht kommen kann, wenn die ursprüngliche Zielsetzung aufgegeben oder in absehbarer Zeit nicht weiterverfolgt wird.

10.5 Krankenhausautomation

Die Krankenhäuser in staatlicher und kommunaler Trägerschaft sind zu rund 90 % an ein landeseinheitliches Verbundsystem der Krankenhaus-Datenverarbeitung angeschlossen, das vom Statistischen Landesamt angeboten wird. Das Verbundsystem ist eingebettet in eine bundesweite kooperative Verfahrensentwicklung, die seit Anfang der 70er Jahre besteht.

Bedingt durch die schnelle technologische Entwicklung im Datenverarbeitungsbereich hat sich das technische Konzept in den seit dem vergangenen rund 20 Jahren erheblich gewandelt. Die ersten Datenverarbeitungsverfahren waren noch ausschließlich stapelorientiert; sie wurden zu bestimmten festen Produktionsterminen im Rechenzentrum des Statistischen Landesamtes zentral durchgeführt. Die günstige Entwicklung des Preis/Leistungsverhältnisses am Rechnermarkt ermöglichte es den Krankenhäusern jedoch bald, in immer stärkerem Umfange Vorortsysteme (Krankenhausrechner) einzusetzen und diese im Verbund mit dem Rechner des Statistischen Landesamtes zu nutzen. Im Laufe der Jahre wurden sukzessive alle Krankenhäuser mit solchen DV-Verfahren ausgestattet. Die derzeitige technische Konzeption stellt sich dar als ein Verbundsystem zwischen dezentraler (Krankenhausrechner) und zentraler (Rechenzentrum des Statistischen Landesamtes) Datenverarbeitung, wobei bestimmte Teilaufgaben selbständig im Krankenhaus wahrgenommen werden. Stapelverarbeitungsorientierte Verfahren der 70er Jahre werden sukzessive auf Dialogverfahren umgestellt, neue Verfahren ausschließlich als Dialogverfahren entwickelt. Ein Teil der Krankenhausrechner ist zusätzlich gekoppelt mit Subsystemen, speziellen Erfassungsgeräten und PCs, die den Krankenhäusern bei Verwendung leistungsfähiger Software Möglichkeiten der individuellen Auswertung und Weiterverarbeitung ihrer Daten eröffnen. Es ist geplant, die geltende Konzeption des Verbundsystems zu einer völlig dezentralen (autonomen) DV-Lösung, basierend auf Rechnern mit dem Betriebssystem UNIX und einem dort verfügbaren Datenbanksystem, weiterzuentwickeln. Dazu wird die Vorort-Software z. Z. auf einem UNIX-System verfügbar gemacht. Auch die Einsetzbarkeit der zentralen Verfahren des Rechnungswesens unter UNIX ist in Vorbereitung.

Das Leistungsangebot umfaßt z. Z. folgende DV-Verfahren:

Vor-Ort-Verfahren (Krankenhausrechner)

- Patientenverwaltung
- Datenerfassung für das kaufmännische Rechnungswesen
- Patientengeldbuchhaltung
- Bearbeitung von Eingangsrechnungen
- Materialwirtschaft (MARK) mit Bestellwesen und Zentralapothekenteil
- Gesetzliche Diagnosenstatistik (GEDI)
- Diagnosendokumentation (DIDOK)
- Geräteverwaltung (MedGV)
- Personalverwaltungssystem (PVS)
- Datenbereitstellung IRIS-Fremdrechner (DAIF)

Hintergrundverfahren

- Stationäre Leistungserfassung und -abrechnung
- Ambulante Leistungserfassung und -abrechnung
- Betriebsstatistiken

Dialogisiertes Rechnungswesen

- Hauptbuchhaltung
- Anlagenbuchhaltung

- Lagerbuchhaltung
- Debitorenbuchhaltung
- Kostenrechnung
- Verwahrgeldbuchhaltung
- Kreditorenbuchhaltung
- Verfahrensübergreifende Funktionen (Buchungsbereiche einschl. „wiederkehrender Buchungen")
- Controlling

Datenschutzrelevant sind insbesondere solche Verfahren, in denen medizinische Daten im engeren Sinne, also beispielsweise Diagnosedaten, verarbeitet werden. Dies ist beispielsweise bei dem Verfahren „Diagnosedokumentation – DIDOK –" der Fall. Die DSK hat die Verfahrensentwicklung, die im wesentlichen bereits 1985 abgeschlossen wurde, beratend begleitet. Sie hat insbesondere auf eine strikte Begrenzung der Zugriffsbefugnisse hingewirkt. Eine Zugriffsbefugnis auf personenbezogene Diagnosedaten steht im Grundsatz nur den behandelnden Ärzten der jeweiligen Fachabteilung zu. Die seinerzeit von der DSK aus dem allgemeinen Arztgeheimnis entwickelten Lösungsvorschläge haben auch vor dem Hintergrund der inzwischen eingetretenen Rechtsentwicklung (Landeskrankenhausgesetz) Bestand.

Neue Probleme birgt der oben erwähnte Einsatz von PC im Krankenhaus. Diese PC können mit dem Krankenhausrechner verbunden oder auch mit anderen PC im Krankenhausbereich vernetzt sein.

Das Verfahrens-DAIF (Datenbereitstellung IRIS-Fremdrechner) bietet die Möglichkeit, Datenbank- und Listeninhalte des Krankenhausrechners – in einer für den File-Transfer verständlichen Form – für die Übertragung in PC bereitzustellen. Über Steueranweisungen können Sätze aus der Datenbank umstrukturiert, selektiert und sortiert werden. Zwar ist das Bereitstellungsverfahren im Krankenhausrechner in der üblichen Weise paßwortgeschützt und die DAIF-Anwendung wird protokolliert; die Daten im PC unterliegen aber den Verarbeitungsbedingungen dieser Rechner und der hierfür realisierten Datensicherung. Diese Datensicherung muß nach den datenschutzrechtlichen Bestimmungen angemessen sein; demzufolge fordert die Möglichkeit der Verarbeitung sehr sensibler Daten – beispielsweise aus der Diagnosedokumentation – den Einsatz einer besonders leistungsfähigen PC-Sicherungssoftware. Die DSK hat die aus ihrer Sicht zu stellenden Anforderungen definiert und den Krankenhäusern mitgeteilt.

10.6 Verweisung im Landeskrankenhausgesetz auf Vorschriften des Bundesdatenschutzgesetzes

§ 36 Abs. 7 des Landeskrankenhausgesetzes (LKG) statuiert für Krankenhausträger die Verpflichtung, einen Beauftragten für den Datenschutz zu bestellen. Bezüglich der Qualifikation, Stellung und Unterstützung des Beauftragten für den Datenschutz verweist das LKG auf § 29 des Bundesdatenschutzgesetzes.

Der LfD sieht diese Verweisung in Übereinstimmung mit dem Ministerium für Arbeit, Soziales, Familie und Gesundheit als statisch an. Als solche hat sie die Wirkung, daß die zitierten Vorschriften in der bisherigen Fassung auch nach dem Inkrafttreten des novellierten und inhaltlich veränderten Bundesdatenschutzgesetzes für den Krankenhausbereich in Geltung bleiben.

Aus Gründen der Rechtsklarheit beabsichtigt das Ministerium, bei der nächstfälligen Fortschreibung des LKG auf die novellierten Bestimmungen des Bundesdatenschutzgesetzes zu verweisen.

Die Novellierung des LKG sollte nach Auffassung des LfD auch genutzt werden, konkrete Bestimmungen darüber zu treffen, ob und ggf. unter welchen Bedingungen die Beauftragten für den Datenschutz in den Krankenhäusern befugt sind, bei der Ausübung ihrer Tätigkeit personenbezogene Behandlungsdaten von Patienten zur Kenntnis zu nehmen.

In Abwägung der Geheimhaltungsinteressen von Patienten mit den Notwendigkeiten der krankenhausinternen Datenschutzkontrolle tritt der LfD, nicht zuletzt im Blick auf die Neuregelung in § 24 Abs. 2 Nr. 2 Buchst. b des Bundesdatenschutzgesetzes, dafür ein, Kontrollen des Krankenhaus-Datenschutzbeauftragten in Bereichen, in denen ihm personenbezogene Behandlungsdaten zur Kenntnis gelangen können, nur mit dem Einverständnis der Patienten zuzulassen. Auch in der Beurteilung dieser Frage besteht im wesentlichen Einvernehmen mit dem zuständigen Ressort.

10.7 Erfahrungsaustausch

Der Erfahrungsaustausch mit den Datenschutzbeauftragten der Krankenhäuser in öffentlicher Trägerschaft – die DSK berichtete hierüber unter Tz. 9.6.2 ihres 12. Tätigkeitsberichts – wurde im Berichtszeitraum fortgesetzt. Im September 1990 fand in Trier eine Sitzung statt, die wiederum ein erfreuliches Echo fand. Nach wie vor wird der Erfahrungsaustausch geprägt durch die Besprechung von Datenschutzfragen, die sich aus der praktischen Arbeit ergeben. Hierfür sind im folgenden zwei Beispiele geschildert:

Ein Datenschutzbeauftragter stellte die Frage, ob die Mitarbeiter der Poststelle eines Krankenhauses durch Dienstanweisung verpflichtet werden können, an das Krankenhaus „zu Händen von Herrn/Frau xy" adressierte Post als Dienstpost der Krankenhausverwaltung auch dann zu übermitteln, wenn es sich sowohl bei dem Absender wie auch bei dem Adressaten um Ärzte handelt. Hierzu wurde die Auffassung vertreten, daß gegen die Dienstanweisung deshalb Bedenken zu erheben sind, weil sie eine gebotene Differenzierung unterläßt. Sie berücksichtigt nicht, daß im Schriftverkehr zwischen Ärzten – anders als im allgemeinen Schriftverkehr der Verwaltung – die namentliche Benennung des Empfängers eine aus dem Arztgeheimnis resultierende Verpflichtung des Absenders darstellt. Es ist in aller Regel nicht davon auszugehen, daß ein in der erwähnten Weise adressierter Brief zur Kenntnis der Verwaltung bestimmt ist. Es handelt sich zwar um Dienstpost; gleichwohl sind die besonderen Geheimhaltungspflichten der Ärzte durch organisatorische Vorkehrungen zu sichern und zu unterstützen. Für die Praxis bedeutet dies, daß die in der erwähnten Weise adressierten Briefe den Ärzten unmittelbar und ungeöffnet zuzuleiten sind.

Zwar befand das LG Arnsberg in einem rechtskräftigen Urteil vom 27. Oktober 1989 – 1 O 367/89 –, daß im Krankenhaus eingehende Briefe, die von einem Arzt „z. H." eines anderen Arztes adressiert sind, von der Poststelle des Krankenhauses geöffnet werden dürfen. Dieses Urteil läßt freilich die Tatsache, daß es sich häufig um Informationsübermittlungen in einem durch das Arztgeheimnis besonders geschützten Bereich handelt, unberücksichtigt. Es hebt darauf ab, daß regelmäßig von einer Einwilligung des absendenden Arztes zur Öffnung der Briefe durch das Krankenhaus auszugehen sei und läßt unberücksichtigt, daß diese Einwilligung nicht weiter reichen kann, als die Einwilligung des betroffenen Patienten in die Offenbarung. Daß ein Arztbrief an die Krankenhausverwaltung gelangt, dürfte in aller Regel vom Patienten nicht gewollt sein.

Eine andere Frage betraf die Zulässigkeit der Speicherung der Zielnummern bei Dienstgesprächen von Krankenhausseelsorgern. Für den Zuständigkeitsbereich der DSK wurde hierzu die Auffassung vertreten, daß es im Grundsatz zulässig ist, bei dienstlichen Telefonaten die vollständige Zielnummer für Kontrollzwecke zu speichern. Zu beachten – und wohl im Ergebnis auf die seelsorgerische Tätigkeit übertragbar – ist indessen die in dem Urteil des Bundesarbeitsgerichts vom 13. Januar 1987 – 1 AZR 267/85 – vertretene Auffassung. Danach darf sich der Arbeitgeber eines in einer Beratungsstelle tätigen Psychologen mit anerkannter wissenschaftlicher Abschlußprüfung die Kenntnis darüber, mit welchen der von diesem zu betreuenden Personen ein Telefongespräch geführt wurde, nicht dadurch verschaffen, daß er die Zielnummer der Telefongespräche erfaßt. Die Praxis, Teile der Zielnummer zu unterdrücken, ist nach Meinung der DSK in aller Regel geeignet, den Zielkonflikt zwischen dem Erfordernis dienstlicher Kontrolle im Interesse der Wirtschaftlichkeit und Sparsamkeit einerseits und Geheimhaltungsinteressen andererseits zu lösen.

10.8 KLIMACS

KLIMACS ist ein Verfahren zur rechnergestützten Krankendokumentation bei HIV-Infizierten. Es zielt auf eine effizientere Bearbeitung und Auswertung anfallender Daten und soll gleichermaßen der Verbesserung der Patientenversorgung wie auch – durch Übermittlung aggregierter Daten an eine Zentralstelle – wissenschaftlichen Zwecken dienen.

Durch Presseberichte erhielt die DSK Kenntnis von dem Verfahren und seiner Anwendung in einer Klinik ihres Kontrollbereichs. Örtliche Feststellungen in dieser Klinik im Dezember 1991 ergaben, daß im Vorgriff auf die Gesamtnutzung von KLIMACS ein Programm eingesetzt wurde, das die Arztbriefschreibung unterstützt. Es waren eine Vielzahl außerordentlich empfindlicher Patientendaten erfaßt und gespeichert. Die DSK forderte, daß die unzureichenden technischen und organisatorischen Datenschutzmaßnahmen wesentlich verbessert werden, insbesondere die Patientenakten und die Sicherungsdisketten in verschließbaren Stahlschränken aufbewahrt und eine Datensicherungssoftware eingesetzt wird, die folgende Leistungsmerkmale aufweist:

- Protokollierung von Benutzeraktivitäten, insbesondere von Kopiervorgängen,
- Online-Verschlüsselung der Festplatte, Kopierschutz durch Verschlüsselung,
- Ausschluß des Zugriffs zur Betriebssystemebene für Benutzer,
- Bootschutz vom Diskettenlaufwerk.

Eine erneute datenschutzrechtliche Prüfung der Anwendung durch Mitarbeiter der Behörde des LfD im Mai 1991 ergab, daß zwar – wie empfohlen – Stahlschränke angeschafft worden waren, im übrigen aber nichts unternommen worden war, um den technischen und organisatorischen Datenschutz zu verbessern. Die Stahlschränke blieben außerhalb der Dienstzeit unverschlossen, die Sicherungsdisketten wurden in einem Pappkarton auf dem Schreibtisch aufbewahrt, eine Datensicherungssoftware war noch immer nicht vorhanden, und es existierte auch keine Dienstanweisung mit näheren Bestimmungen über die konkret zu beachtenden technischen und organisatorischen Datensicherungsvorkehrungen.

Der Klinikleiter hat aufgrund der nachdrücklichen Aufforderung, unverzüglich eine den gesetzlichen Bestimmungen entsprechende Datensicherung zu realisieren, mitgeteilt, daß nunmehr das Erforderliche veranlaßt worden sei.

10.9 Neonatologische Erhebung in Rheinland-Pfalz

Seit dem Jahre 1985 werden in Rheinland-Pfalz Daten über den Gesundheitszustand von Schwangeren und den Verlauf von Entbindungen an eine Dokumentationszentrale bei der Kassenärztlichen Vereinigung Trier übermittelt und dort in automatisierten Verfahren mit dem Ziel ausgewertet, Erkenntnisse zu gewinnen, die für eine qualitative Verbesserung der ärztlichen Behandlung genutzt werden können. Über Datenschutzprobleme im Zusammenhang mit dieser sog. Perinatologischen Basiserhebung berichtete die DSK in ihrem Zehnten Tätigkeitsbericht unter Tz. 9.3 und in ihrem Zwölften Tätigkeitsbericht unter Tz. 9.7.

Neuerdings wird diese Erhebung und Verarbeitung perinatologischer Daten durch die Erhebung und Verarbeitung neonatologischer Daten – dies sind Gesundheitsdaten von Neugeborenen – ergänzt. Kinderkliniken und Kinderabteilungen von Krankenhäusern übermitteln derartige Daten ebenfalls an die Dokomentationszentrale; dort werden sie mit den perinatologischen Daten verknüpft und ausgewertet. Die Zustimmung der Eltern zur Offenbarung der Daten durch die Krankenhausärzte wird nicht eingeholt. Durchschriften des Neonatologischen Erhebungsbogens, der eine Vielzahl empfindlicher Daten enthält, werden an die Geburtsklinik und an den nachbehandelnden Arzt weitergegeben.

Im datenschutzrechtlichen Sinne ist die Neonatalerhebung als qualitätssichernde Maßnahme anzusehen. Für derartige Maßnahmen dürfen nach § 36 Abs. 3 Nr. 4 Landeskrankenhausgesetz Daten übermittelt werden, wenn das Interesse der Allgemeinheit an der Durchführung die schutzwürdigen Belange des Patienten deutlich überwiegt. Die DSK ging davon aus, daß diese gesetzlichen Voraussetzungen vorliegen.

Die Datenübermittlungen an die Geburtsklinik und an den nachbehandelnden Arzt indessen dienen nicht der Neonatalerhebung, sondern allenfalls der Durchführung des Behandlungsvertrages einschließlich der Nachbehandlung. Solche Datenübermittlungen sind nach den Bestimmungen des LDatG nur zulässig, wenn sie erforderlich sind. Die Erforderlichkeit muß in jedem Einzelfall beurteilt werden. Außerdem darf die Übermittlung nur dann erfolgen, wenn der Patient, in Ausnahmefällen möglicherweise auch sein gesetzlicher Vertreter, nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt.

In einem Gespräch sagten Vertreter des Ministeriums für Arbeit, Soziales, Familie und Gesundheit zu, daß die Krankenhausträger über die Voraussetzungen der Datenübermittlung und die Hinweispflichten durch ein Rundschreiben informiert werden. Dem LfD fiel die Aufgabe zu, dem Ministerium einen Formulierungsvorschlag für einen Text vorzulegen, der als Hinweis in die Aufnahmeerklärung aufgenommen oder den Patienten gesondert zur Kenntnis gebracht wird.

10.10 Onkologisches Nachsorgeprogramm Rheinland-Pfalz

Das Onkologische Nachsorgeprogramm verfolgt zwei Ziele:

- Die ambulante ärztliche Versorgung von Tumorkranken, die aus stationärer Behandlung entlassen wurden, soll dadurch verbessert werden, daß die Patienten durch eine bei der Kassenärztlichen Vereinigung Trier gebildete Nachsorgeleitstelle regelmäßig aufgefordert werden, Nachsorgeuntersuchungstermine wahrzunehmen.

- Die bei Nachsorgeuntersuchungen gewonnen Daten sollen im Tumorzentrum Rheinland-Pfalz e. V., Mainz, wissenschaftlich bearbeitet werden mit dem Ziel, durch Langzeitdarstellung von Krankheitsverläufen und deren Auswertung Hinweise für eine erfolgreichere Behandlung von Tumorerkrankungen zu gewinnen.

Geplant ist folgendes Verfahren: Die vom Arzt erfaßten Behandlungsdaten werden an die jeweils zuständige Kassenärztliche Vereinigung (KV) übermittelt, die die Ordnungsmäßigkeit und Vollständigkeit für Zwecke der Honorarabrechnung überprüft. Nach der Weiterübermittlung der Daten an die Nachsorgeleitstelle werden dort die für eine termingerechte Einbestellung der Patienten zu Nachsorgeuntersuchungen erforderlichen Daten gespeichert und für den genannten Zweck verwendet. Im Anschluß werden die Dokumentationsbögen an das Tumorzentrum e. V. Mainz weitergeleitet, dem die wissenschaftliche Bearbeitung obliegt.

Die ausdrückliche Einwilligung der Patienten in die Erhebung und weitere Verarbeitung der Daten wurde vom LfD als Zulässigkeitsvoraussetzung anerkannt. Dabei wurde berücksichtigt, daß der Gesetzgeber in Rheinland-Pfalz – anders als beispielsweise im Saarland – keine Verfahrensbestimmungen für Krebsregister und insbesondere keine Festlegung hinsichtlich der Registerstelle, der es alleine vorbehalten ist, personenbezogene Daten über Krebspatienten zu verarbeiten, getroffen hat. Wäre dies der Fall, käme – wie im Saarland – eine Verarbeitung der Daten von Krebspatienten außerhalb der Registerstelle auch mit Zustimmung der Betroffenen nicht in Betracht.

Unklar war indessen zunächst, welchen gesetzlichen Bestimmungen die Aufgabenzuweisung zur Durchführung des Nachsorgeprogramms an die KV zu entnehmen ist. In Betracht kam § 75 Abs. 6 SGB V, der es den Kassenärztlichen Vereinigungen erlaubt, mit Zustimmung der Aufsichtsbehörde weitere Aufgaben der ärztlichen Versorgung zu übernehmen. Der Minister für Arbeit, Soziales, Familie und Gesundheit vertrat die Auffassung, daß diese Bestimmung es der Kassenärztlichen Vereinigung ermöglicht, die im Rahmen des Onkologischen Nachsorgeprogramms Rheinland-Pfalz vorgesehenen Aufgaben zu übernehmen. Die Terminierung der Nachsorgeuntersuchungen für Tumorpatienten und die Kontrolle der Rücklaufbögen könne als Bestandteil der ärztlichen Behandlung im Sinne des § 73 Abs. 2 Nr. 1 SGB V angesehen werden. Er beabsichtige, die Zustimmung entsprechend § 75 SGB V zu erteilen.

Der LfD hat diese Rechtsauffassung akzeptiert. Er wies auf die Notwendigkeit hin, zwischen den übrigen an dem Projekt beteiligten Kassenärztlichen Vereinigungen und der Kassenärztlichen Vereinigung Trier ein Auftragsverhältnis im Sinne des § 88 SGB X zu begründen. Im übrigen empfahl er, die Betroffenen deutlich darauf hinzuweisen, daß sie, auch wenn sie die Einwilligung zur Teilnahme an dem Einladungsverfahren nicht erteilen, im gesetzlich bestimmten Umfange ärztliche Leistungen in Anspruch nehmen können.

Schließlich hielt er es für geboten, in seiner Stellungnahme an das Ministerium anzumerken, daß mit der Nachsorge-Datenbank ehemaliger Krebspatienten bei der Kassenärztlichen Vereinigung Trier nach der Perinatal- und Neonataldatenbank das dritte zentrale Register mit sehr empfindlichen Daten aus dem medizinischen Bereich entsteht. Diese Konzentration verstärkt die Datenschutzrisiken, die grundsätzlich auch dann vorhanden sind, wenn eine Datenverarbeitung gesetzlich zugelassen ist. Der LfD sieht das Erfordernis, mit besonderer Sorgfalt die Einhaltung der gesetzlichen Bestimmungen über den Persönlichkeitsschutz zu überwachen und geht davon aus, daß er hierbei durch die Aufsichtsbehörde unterstützt wird. Die Übernahme weiterer zentraler Aufgaben durch diese KV wird unter datenschutzpolitischen Gesichtspunkten als bedenklich angesehen.

10.11 Angabe der Facharztbezeichnung auf Arbeitsunfähigkeitsbescheinigungen

Eine Kassenärztliche Vereinigung erbat die Stellungnahme des LfD zu der Frage, ob es zulässig ist, auf Arbeitsunfähigkeitsbescheinigungen zur Vorlage beim Arbeitgeber die Facharztbezeichnung anzugeben. Sie verwies auf die einerseits nach der Berufsordnung für die Ärzte bestehende Pflicht (§§ 27 und 29), die Arztbezeichnung nach der Weiterbildungsordnung – wie z. B. Arzt für Psychiatrie, Urologe – durch Stempelaufdrucke oder in Briefbögen anzugeben, und auf die andererseits mit dieser Verfahrensweise zwangsläufig verbundene Offenbarung einer Information zur Art der Erkrankung.

Der Bitte wurde entsprochen, obwohl der LfD für die freipraktizierenden Ärzte, die der Kassenärztlichen Vereinigung angehören, keine Kontrollzuständigkeit hat. Er ist aber für Krankenhäuser in öffentlicher Trägerschaft zuständig und entnahm, weil das Problem in diesem Bereich ebenso entstehen kann, hieraus die Legitimation zur Äußerung.

Eine nähere Befassung mit der Thematik führt zu dem Ergebnis, daß es im Grundsatz nicht in einer für den Patienten befriedigenden Weise lösbar ist. Dies ergibt sich aus folgendem: Die Verpflichtung, die Arbeitsunfähigkeit gegenüber dem Arbeitgeber oder Dienstherrn innerhalb einer bestimmten Frist nachzuweisen, besteht gleichermaßen für Arbeiter (§ 3 LohnfortzG), Angestellte (z. B. § 18 Abs. 3 BAT) und Beamte (aufgrund des besonderen Dienst- und Treueverhältnisses). Dieser Nachweis ist durch Vorlage der Bescheinigung eines Arztes zu führen. Name, Anschrift und Unterschrift des ausstellenden Arztes sind unverzichtbare Bestandteile einer solchen Bescheinigung. Selbst wenn die Arztbezeichnung nicht angegeben oder unkenntlich gemacht ist, wird der Arbeitgeber in der Lage sein, sich aus allgemein zugänglichen Quellen – Fernsprechbuch, Ärztehandbuch – Gewißheit darüber zu verschaffen, welche Arztbezeichnung der ausstellende Arzt führt. Die Feststellung der prinzipiellen Unlösbarkeit des Problems präjudiziert freilich nicht die Rechtsverhältnisse zwischen dem Betroffenen und seinem Arbeitgeber bzw. Dienstherrn einerseits und zwischen dem Patienten und dem behandelnden Arzt andererseits.

Der Inhalt der Arbeitsunfähigkeitsbescheinigung bezieht sich, von den obigen Angaben abgesehen, auf die Arbeitsverhinderung und ihre voraussichtliche Dauer. Keine Mitteilungspflicht besteht – von Sonderfällen abgesehen – wegen der Krankheitsart oder der Krankheitssymptome (vgl. Schaub, Arbeitsrechtshandbuch, S. 646). Eine Verpflichtung, dem Arbeitgeber die Arztbezeichnung zur Kenntnis zu bringen, besteht weder nach gesetzlichen noch tarifvertraglichen Bestimmungen und nach Auffassung des LfD auch nicht als arbeitsvertragliche Nebenpflicht.

Die Verpflichtung des Arztes, seinem Patienten bei Arbeitsunfähigkeit eine Bescheinigung darüber auszustellen, besteht aufgrund des Behandlungsvertrags. Die in der Berufsordnung für die Ärzte festgelegten Pflichten sind Vertragsbestandteile (vgl. Müller, K.: Schweigepflicht und Schweigerecht des Arztes, in Mergen, A.: Die juristische Problematik in der Medizin, Bd. II, München, 1971, S. 99). Zu diesen Pflichten gehört auch die Beachtung des § 2, der dem Arzt die Verpflichtung zur Wahrung des Arztgeheimnisses auferlegt.

Unstreitig ist bereits die Tatsache eines Arztbesuchs als Information durch § 2 der Berufsordnung geschützt und die unbefugte Offenbarung durch § 203 StGB strafbewehrt. Ein Arzt, der seinem Patienten eine Bescheinigung zur Vorlage bei dessen Arbeit-

geber ausstellt, wird zu berücksichtigen haben, daß – in aller Regel zwar nicht unmittelbar, aber doch unter Einschaltung des Patienten – geschützte Informationen offenbart werden. Da der Patient seinen vertraglichen oder dienstrechtlichen Obliegenheiten nur durch Vorlage einer ärztlichen Bescheinigung genügen kann, wird der Arzt, weil es um die Offenbarung von Patientendaten geht, jedenfalls dem Wunsch des Patienten entsprechen müssen, keine entbehrlichen Informationen in die Bescheinigung aufzunehmen.

Es bestehen keine Bedenken, davon auszugehen, daß der Arzt die konkludente Einwilligung des Patienten in die Verwendung eines Vordrucks oder Stempels mit genauer Arztbezeichnung unterstellen kann, wenn der Patient nichts anderes bestimmt. Dies um so mehr, als er von einer verhältnismäßig geringen Schutzfähigkeit der Information ausgehen kann, weil der Arbeitgeber/die Dienstbehörde die Arztbezeichnung in Erfahrung bringen kann, wenn daran Interesse besteht. Widerspricht aber ein Patient der Angabe der Arztbezeichnung, so wird der Arzt prüfen müssen, ob für die Offenbarung, weil die Zustimmung als Rechtfertigungsgrund ausscheidet, ein anderer Rechtfertigungsgrund besteht. Dies ist nicht der Fall. §§ 27 und 28 der Berufsordnung scheiden als Rechtsgrundlage einer Offenbarung aus, weil die Ärztekammer durch Satzungsrecht nur die Rechte und Pflichten ihrer Mitglieder regeln und nicht in Rechte Dritter, also der Patienten, eingreifen kann.

Auch auf den Bundesmantelvertrag als Vertragsrecht zwischen den Leistungserbringern können Eingriffsbefugnisse in das informationelle Selbstbestimmungsrecht der Patienten nicht gestützt werden.

11 Sozialleistungsbereich

11.1 Krankenversicherung

11.1.1 Angabe von Diagnosen auf Krankenscheinen

In der Ärzteschaft, zwischen den Vertragspartnern im Krankenversicherungsbereich, im Kreis der Datenschutzbeauftragten des Bundes und der Länder und in der Öffentlichkeit wurde die Frage diskutiert, ob es aufgrund der Bestimmungen des „Gesundheitsreformgesetzes" (Fünftes Buch des Sozialgesetzbuchs, SGB V) noch zulässig ist, auf den für die Abrechnung ärztlicher Leistungen bestimmten Krankenscheinen die Diagnose anzugeben. Vor dem Inkrafttreten des Gesundheitsreformgesetzes war diese Praxis allgemein als zulässig angesehen worden. Aufgrund der Änderung des Rechts der gesetzlichen Krankenversicherung waren Bedenken hiergegen insbesondere deshalb geäußert worden, weil die Diagnose als übermittlungsfähiges Datum in der die Abrechnung ärztlicher Leistungen regelnden Vorschrift (§ 295 SGB V) nicht ausdrücklich genannt ist.

Diese Bedenken werden u. a. gestützt durch den Hinweis auf die Detailgenauigkeit anderer Vorschriften, insbesondere des § 301 SGB V, der die Übermittlung sowohl der Aufnahmediagnose wie auch der Entlassungsdiagnose durch Krankenhäuser an Krankenkassen ausdrücklich zuläßt. Demgegenüber argumentierten die Verbände der Vertragspartner und der Bundesminister für Arbeit und Sozialordnung, daß die Diagnoseangabe auf den Abrechnungsunterlagen Bestandteil einer ordnungsmäßigen Leistungsbeschreibung sei, die nach dem Willen des Gesetzgebers beibehalten werden sollte. Im übrigen wird auf die Erforderlichkeit der Diagnoseangaben für die Durchführung von Wirtschaftlichkeits-, Plausibilitäts- und Qualitätskontrollen hingewiesen, ungeachtet des von der Datenschutzseite vertretenen Standpunkts, daß hierfür nur Datenübermittlungen im Einzelfalle und nicht die routinemäßige Übermittlung von Diagnosen in jedem Abrechnungsfalle erforderlich sind.

Die DSK brachte in einer Stellungnahme zum Ausdruck, daß sie die Bestrebungen, mit der Ergänzung des § 295 Abs. 1 SGB V eine jeglichen Zweifel ausschließende Rechtsgrundlage für die in Rede stehende Datenübermittlung unter strikter Beachtung des Erforderlichkeitsprinzips zu schaffen, unterstützt. Sie hielt indessen die Datenübermittlung auch auf der Grundlage der gegenwärtigen Fassung des § 295 SGB V für zulässig, weil die erbrachte Leistung allein durch die Aufzeichnung der Gebührenposition in den Abrechnungsunterlagen häufig nicht hinreichend deutlich beschrieben ist.

11.1.2 Maßnahmen der Gesundheitsförderung und Krankheitsverhütung

In ihrem 12. Tätigkeitsbericht äußerte die DSK unter Tz. 12.2 Bedenken gegen die Erhebung und Verarbeitung von Verhaltensdaten oder sonstigen Informationen über Versicherte zu dem Zweck, diesen in einem „Einladungsverfahren" Leistungen zur Früherkennung von Krankheiten (§§ 25 und 26 SGB V) anzubieten. Im Berichtszeitraum wurden erneut Vorgänge bekannt, die die Erhebung von Daten für Früherkennungsmaßnahmen und die Zweckentfremdung von Abrechnungsdaten betrafen. So wurde beispielsweise ein Patient aufgefordert, zum Zwecke einer Diabetesberatung vierteljährlich eine Kontrolle des HBA-1-Wertes vornehmen zu lassen und das Ergebnis seiner Krankenkasse mitzuteilen.

Offensichtlich gehen einzelne Krankenkassen davon aus, daß ihnen durch das Gesundheitsreformgesetz Befugnisse zugewachsen sind, die weit in das Arzt-Patientenverhältnis hineinreichen. Der LfD ist ebenso wie die DSK der Auffassung, daß § 20 SGB V den Krankenkassen keine Befugnis gibt, zum Zwecke der Aufklärung über Maßnahmen der Gesundheitsförderung und Krankheitsverhütung Gesundheitsdaten von Versicherten zu erheben und zu speichern oder Abrechnungsdaten hierfür zu ver-

wenden, denn Aufgabe der Krankenkassen ist nach der genannten Vorschrift lediglich die „allgemeine" Aufklärung. Danach sind Aufklärungsmaßnahmen weder als Pflichtleistung noch als Ermessensleistung zugelassen, wenn sie die Erhebung und Aufzeichnung von Daten über das Verhalten oder den Gesundheitszustand einzelner Versicherter oder eine Zweckentfremdung von Abrechnungsdaten zur Voraussetzung haben.

11.1.3 Zulässigkeit der Datenspeicherung über geringfügig Beschäftigte bei Krankenkassen

Eine der Kontrollzuständigkeit der DSK unterliegende Krankenkasse fragte an, ob es zulässig sei, die nach § 105 Abs. 3 SGB IV an die Datenstelle der Rentenversicherungsträger zu übermittelnden Meldungen für geringfügig Beschäftigte auch für Prüfzwecke der Krankenkassen zu speichern. Die Kasse vertrat die Auffassung, daß die Speicherung in einer eigenen Datei erforderlich sei, damit sie ihrer Prüfungspflicht bei den Arbeitgebern nachkommen könne.

Die DSK wies in ihrer Stellungnahme darauf hin, daß § 105 Abs. 3 SGB IV detailliert regelt, was mit den Meldungen für geringfügig Beschäftigte zu geschehen hat. Eine Speicherung der Meldungen durch die Einzugsstellen ist danach nicht vorgesehen. Demgegenüber weist das Gesetz der Datenstelle der Rentenversicherungsträger, an die die Daten von der Einzugsstelle zu übermitteln sind, ausdrücklich eine Speicherungsbefugnis zu. Eine Prüfung von Beschäftigungsverhältnissen durch die Einzugsstellen auf der Grundlage der Meldungen nach § 104 SGB IV ist nur dann zulässig, wenn sie von der Datenstelle der Rentenversicherungsträger veranlaßt wird.

Das Ministerium für Soziales und Familie bestätigte diese Rechtsauffassung und unterrichtete die seiner Aufsicht unterstehenden Krankenkassenverbände.

11.1.4 Amtshilfe für Bundespost und Telekom

Die DSK äußerte sich auf Ersuchen von Krankenversicherungsträgern wiederholt zur Zulässigkeit der Offenbarung von Sozialdaten – insbesondere Angabe des Arbeitgebers – an Fernmeldeämter. Diese begründeten die Amtshilfeersuchen mit der Notwendigkeit, Vollstreckungsmaßnahmen durchzuführen, und wiesen darauf hin, daß es mit den im Rahmen des Verwaltungsvollstreckungsverfahrens verfügbaren Maßnahmen nicht möglich war, den Arbeitgeber zu ermitteln.

Demgegenüber verwiesen die Krankenkassen auf die Subsidiaritätsregelung des § 68 SGB X. Danach ist Amtshilfe nur zulässig, wenn sich die ersuchende Stelle die Angaben nicht auf andere Weise beschaffen kann. Den Fernmeldeämtern sei zuzumuten, die Schuldner zur eidesstattlichen Darlegung ihrer Vermögensverhältnisse zu zwingen und aufgrund der so gewonnenen Erkenntnisse weitere Maßnahmen einzuleiten.

Die DSK vertrat demgegenüber die Auffassung, daß auch der Subsidiaritätsgrundsatz des § 68 SGB X dem Verfassungsgebot der Verhältnismäßigkeit entsprechen muß. Im Rahmen der Verhältnismäßigkeitsprüfung sei insbesondere die für den Betroffenen mit der Informationsbeschaffung – Eidesstattliche Versicherung – verbundene Belastung zu berücksichtigen. Sie hielt es nicht für angemessen, von der ersuchenden Stelle – Fernmeldeamt – zu verlangen, daß die Arbeitgeberdaten im Offenbarungseidverfahren ermittelt werden.

Zugleich wies sie aber darauf hin, daß auch bei der Prüfung, ob die Voraussetzungen für ein Amtshilfeersuchen vorliegen, der Verhältnismäßigkeitsgrundsatz zu beachten ist. Eine Durchbrechung des Sozialgeheimnisses im Rahmen einer Amtshilfeleistung nach § 68 SGB X könne beispielsweise dann nicht in Betracht kommen, wenn der zu vollstreckende Geldbetrag nur gering sei. Dies sei von den Fernmeldeämtern bei der Prüfung der Zulässigkeit eines Amtshilfeersuchens zu berücksichtigen.

Aufgrund der Umstrukturierung der Deutschen Bundespost besteht Veranlassung, die von der DSK vertretene Rechtsauffassung zu überprüfen. Es stellt sich nämlich die Frage, ob die Deutsche Bundespost – Telekom überhaupt Behörde i. S. des § 1 Abs. 2 SGB X und damit amtshilfeberechtigt ist. Dies ist zumindest insoweit zu verneinen, als im Zusammenhang mit der Inanspruchnahme der Einrichtungen der Deutschen Bundespost Telekom Rechtsbeziehungen entstehen, die nach § 9 Fernmeldeanlagengesetz privatrechtlicher Natur sind.

Die zu dieser Frage zwischen den Datenschutzbeauftragten des Bundes und der Länder in Gang gekommene Diskussion ist noch nicht abgeschlossen.

11.2 Medizinischer Dienst der Krankenversicherung

Der Medizinische Dienst der Krankenversicherung (MDK) wurde durch das Gesundheitsreformgesetz (SGB V) mit Wirkung vom 1. Januar 1990 als Arbeitsgemeinschaft und rechtsfähige Körperschaft eingeführt. Er trat an die Stelle des Vertrauensärztlichen Dienstes, der den Landesversicherungsanstalten als unselbständige Abteilung zugeordnet war. Mitglieder der Arbeitsgemeinschaft sind die Landesverbände der Orts-, Betriebs- und Innungskrankenkassen, die Landwirtschaftlichen Krankenkassen und die Verbände der Ersatzkassen.

Der MDK hat die Aufgabe, für die Krankenkassen Gutachten über das Vorliegen der Voraussetzungen sowie Art und Umfang von Leistungen zu erstellen. Seine Beteiligung kommt ferner in Betracht bei der Beurteilung von Arbeitsunfähigkeit, bei der Prüfung, ob Schwerpflegebedürftigkeit vorliegt, oder bei der Prüfung der Voraussetzungen von Kurmaßnahmen. Darüber hinaus sollen die Krankenkassen den MDK zu Rate ziehen, wenn es um allgemeine medizinische Fragen der gesundheitlichen Versorgung und Beratung der Versicherten geht.

Die Datenverarbeitung durch den MDK ist nur in einem verhältnismäßig engen Rahmen zulässig. Nach § 276 Abs. 2 SGB V darf er personenbezogene Daten nur erheben und erfassen, soweit dies für seine Prüfungs-, Beratungs- und Gutachtentätigkeit erforderlich ist. Die Daten unterliegen einer Zweckbegrenzung und sind nach fünf Jahren zu löschen. In Dateien darf der MDK nur Angaben zur Person und Hinweise auf bei ihm vorhandene Akten aufnehmen.

Der MDK Rheinland-Pfalz erbat eine Stellungnahme zu der Frage, ob die fünfjährige Löschungsfrist für Materialien, die vom Vertrauensärztlichen Dienst übernommen wurden, mit dem Ende des Entstehungsjahres dieser Materialien oder mit dem Gründungszeitpunkt des MDK (1. Januar 1990) zu laufen begann. Der LfD vertrat die Auffassung, daß eine Auslegung des § 276 Abs. 2 SGB V nach Sinn und Zweck – Verbesserung des Datenschutzes der Betroffenen – für die Annahme spricht, daß die Löschungsfrist nicht erst mit der Gründung des MDK begann, sondern unter Berücksichtigung des § 304 Abs. 1 SGB V mit dem Ende des Geschäftsjahres, in dem die Prüfung, Beratung oder gutachtliche Stellungnahme erfolgte. Im übrigen ist der Auffassung zuzustimmen, daß, wenn der MDK im Rahmen einer zeitlich gestreckten Leistungsgewährung tätig wurde, die Fünfjahresfrist mit dem Ende des Geschäftsjahres beginnt, in dem die zeitlich gestreckte Gesamtleistung beendet wurde. Gleiches gilt beispielsweise für Stammdaten von Versicherten, bei denen für die Berechnung der Löschungsfrist vom Zeitpunkt der zuletzt erbrachten Leistung auszugehen ist (vgl. Podlech, Kurzgutachten zur Aufbewahrung von Akten im Medizinischen Dienst, Darmstadt, April 1990).

Sofern eine Beeinträchtigung der Belange von Versicherten durch die fristgemäße Löschung von Daten oder Vernichtung von Akten nicht auszuschließen ist, sollte in Betracht gezogen werden, den Versicherten nach Ablauf der Frist die für sie wichtigen Originalbefunde zu übergeben. Damit wäre einerseits dem gesetzgeberischen Anliegen der Löschung Rechnung getragen. Andererseits könnte der Versicherte, wenn es im Einzelfall in seinem Interesse liegt, auf die Informationen zurückgreifen.

Ein anderes Thema, das zwischen den Personalräten der MDK und den Geschäftsführungen kontrovers diskutiert wird, ist Gegenstand der Berichterstattung unter Tz 17.7.

11.3 Sozial- und Jugendhilfe

11.3.1 Kinder- und Jugendhilfegesetz (KJHG)

Das KJHG ist zum Jahresbeginn 1991 in Kraft getreten. Es trägt Datenschutzanforderungen weitgehend Rechnung; in einem gesonderten Kapitel sind bereichsspezifische Datenschutzregelungen zusammengefaßt.

Im einzelnen wurden geregelt:

- der Anwendungsbereich der Datenschutzvorschriften,
- die Datenerhebung, insbesondere der Grundsatz, daß personenbezogene Daten beim Betroffenen zu erheben sind, es sei denn, daß einer der enumerativ genannten Ausnahmefälle vorliegt,
- die Datenspeicherung in Akten und auf sonstigen Datenträgern,
- die Zusammenführung von Daten, die für unterschiedliche Zwecke erhoben wurden,
- die Einschränkung der Offenbarungsbefugnis für solche Daten, die zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind,
- die Datenlöschung und Datensperrung,
- das Auskunfts- und Einsichtsrecht der Betroffenen,
- der Datenschutz im Bereich der Amtspflegschaft und Amtsvormundschaft.

11.3.2 Organisationsuntersuchungen bei Sozialleistungsträgern

Im Rahmen von Organisationsuntersuchungen wird geprüft, ob Aufgaben der öffentlichen Verwaltung mit geringerem Personal- und Sachaufwand oder auf andere Weise wirksamer erfüllt werden können. Dem Rechnungshof sind entsprechende Prüfungsaufgaben durch §§ 88 ff. Landeshaushaltsordnung, den kommunalen Rechnungsprüfungsämtern durch § 50 Landkreisordnung und § 112 Gemeindeordnung übertragen.

Erfordert die Durchführung von Organisationsuntersuchungen bei Sozialämtern oder Jugendämtern die Beiziehung von Leistungsakten – etwa zu dem Zweck, dem Prüfer die Beurteilung der zeitlichen Inanspruchnahme von Bediensteten durch die Sachbearbeitung zu ermöglichen –, stellt sich die Frage, ob und ggf. inwieweit eine Offenbarungsbefugnis besteht. Eine Offenbarung von Sozialdaten ist ohne Einwilligung der Betroffenen nur zulässig, soweit hierfür nach den §§ 68 bis 77 SGB X eine ausdrückliche Befugnis besteht.

Der LfD vertrat auf eine entsprechende Anfrage die Auffassung, daß die Offenbarung von Sozialdaten für die Durchführung von Organisationsprüfungen an Rechnungsprüfungsbehörden im Grundsatz nach § 69 Abs. 2 Nr. 1 SGB X zulässig ist. Diese Vorschrift stellt rechnungsprüfungsberechtigte Behörden bezüglich der Erfüllung gesetzlicher Aufgaben den in § 35 SGB I genannten Stellen – also Sozialleistungsträgern – gleich. Es besteht also eine Offenbarungsbefugnis, wenn die Rechnungsprüfungsbehörde sozialrechtliche Aufgaben zu erfüllen hat.

Für die gesamte staatliche und kommunale Verwaltung und damit auch für die Sozialverwaltung gilt die Verpflichtung zu wirtschaftlichem und sparsamem Handeln. Die Erfüllung von Aufgaben nach dem Sozialgesetzbuch erfordert gleichermaßen die Beachtung der Vorschriften dieses Gesetzbuchs wie auch der allgemeinen Haushaltsgrundsätze. Daß der Gesetzgeber in diesem Rahmen auch die Prüfung der Wirtschaftlichkeit der Sozialverwaltung als sozialrechtliche Aufgabe ansieht, verdeutlicht das Gesundheitsreformgesetz (SGB V), das hierzu eine Fülle von Detailregelungen enthält.

Soweit der Rechnungshof und die kommunalen Rechnungsprüfungsämter aufgrund verfassungsrechtlicher und gesetzlicher Vorschriften Prüfungsaufgaben im Sozialleistungsbereich wahrnehmen, erfüllen sie zugleich auch sozialrechtliche Aufgaben. Dabei besteht kein prinzipieller Unterschied zwischen Organisationsuntersuchungen und der inhaltlichen Überprüfung von Einzelvorgängen, denn die Pflicht zur wirtschaftlichen und sparsamen Haushaltsführung besteht gleichermaßen beim Personaleinsatz wie auch bei der Sachbearbeitung.

Eingegrenzt wird die Offenbarungsbefugnis durch den Grundsatz der Erforderlichkeit (§ 69 Abs. 1). Wenn es zur Durchführung des Prüfungsauftrags bei Organisationsuntersuchungen genügt, anonymisierte Aktenteile oder anonymisierte Kopien aus Akten zu verwenden, so ist die Offenbarung personenbezogener Sozialdaten zur Aufgabenerfüllung nicht erforderlich und demzufolge nicht zulässig.

Hinzuweisen ist in diesem Zusammenhang auch auf den Grundsatz der Zweckbindung und auf die Geheimhaltungspflicht der Empfänger von Sozialdaten (§ 78 SGB X). Die für Prüfungszwecke offenbarten Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie befugt offenbart worden sind. Im übrigen haben Rechnungsprüfungsbehörden die Daten in demselben Umfang geheimzuhalten wie der offenbarende Sozialleistungsträger selbst.

Die ausdrückliche Gleichstellung der „rechnungsprüfungsberechtigten Behörden" mit Sozialleistungsträgern sowohl in § 35 Abs. 1 SGB I wie auch in § 69 Abs. 2 SGB X verdeutlicht aber auch, daß der Gesetzgeber nur diese Behörden als berechtigte Übermittlungsempfänger für Sozialdaten zum Zwecke der Durchführung von Prüfungsaufgaben im Blick hatte. Die Offenbarung von Sozialdaten an externe Prüfungs- und Beratungsunternehmen ist nicht zulässig. Diesen dürfen für die Aufgabenwahrnehmung nur anonymisierte Aktenteile, anonymisierte Kopien und ähnliches zur Verfügung gestellt werden.

11.3.3 Verwendung von Vordrucken im Sozialleistungsverfahren

Die inhaltliche Gestaltung von Vordrucken, die im Sozialleistungsverfahren Verwendung finden, wird immer wieder in Eingaben beklagt. Erklärungen zur Entbindung von der ärztlichen Schweigepflicht oder zur Erteilung von Bankauskünften werden beispielsweise mit dem Sozialhilfeantrag verbunden und sind inhaltlich so unbestimmt, daß sie, wäre die Zustimmungserklärung rechtswirksam, für allgemeine Rundfragen bei Ärzten oder Kreditinstituten genutzt werden könnten. Bisweilen wird dem Antragsteller zugleich die Zustimmung zur Nichtbeachtung datenschutzrechtlicher Vorschriften durch die übermittelnden Stellen abverlangt. Die Kosten einer Auskunftserteilung hat er „selbstverständlich" selbst zu tragen und es wird auch kein rechtliches Problem gesehen, die Zustimmung des Antragstellers auf Sozialleistungen für die Erteilung von Auskünften über unterhaltsberechtigte Angehörige einzuholen.

Wie die DSK weist auch der LfD die Sozialleistungsträger darauf hin, daß pauschale Schweigepflichtentbindungsklauseln wegen fehlender Bestimmtheit rechtlich unwirksam sind. Einwilligungserklärungen können von dem Hilfeempfänger nur in

Kenntnis eines konkreten Anlasses für einen Ermittlungsbedarf erteilt werden. Die Entbindung vom Bankgeheimnis muß den Adressaten (offenbarungsbefugtes Institut), den Umfang der zu offenbarenden Informationen und den Zeitraum, auf den sich die Offenbarungsbefugnis erstrecken soll, benennen. Es genügt nicht, eine pauschale Vollmacht vom Antragsteller unterschreiben zu lassen und ihn dann zu informieren, welche Institute angeschrieben und welche Informationen benötigt werden. Ähnlich ist es bezüglich der Entbindung von der ärztlichen Schweigepflicht. Selbstverständlich kann ein Sozialleistungsträger oder eine übermittelnde Stelle von einem Antragsteller oder Hilfeempfänger nicht von der Pflicht zur Einhaltung datenschutzrechtlicher Vorschriften entbunden werden und die Zustimmung zur Auskunftserteilung über Dritte kann nur im Rahmen einer gesetzlichen oder rechtsgeschäftlichen Vertretungsbefugnis erteilt werden.

11.3.4 Auskünfte über den Arbeitsverdienst

Sozialleistungsträger sind bei der Erhebung von Informationen über die Einkommens- und Vermögensverhältnisse von Sozialleistungsempfängern, Unterhaltspflichtigen und Kostenersatzpflichtigen durch eine Reihe von Vorschriften privilegiert. §§ 116 Abs. 2 Bundessozialhilfegesetz zum Beispiel verpflichtet die Arbeitgeber, dem Träger der Sozialhilfe über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des bei ihm beschäftigen Hilfesuchenden oder Hilfeempfängers, Unterhaltspflichtigen oder Kostenersatzpflichtigen Auskunft zu geben, soweit die Durchführung des Gesetzes dies erfordert. Auskunftspflichten des Arbeitgebers werden ferner durch § 98 SGB X für den Bereich der Sozialversicherung, einschließlich der Arbeitslosenversicherung, begründet.

Die unmittelbare Einholung von Auskünften beim Arbeitgeber durch einen Sozialleistungsträger geht zwangsläufig mit einer Offenbarung von Sozialdaten einher: Der Arbeitgeber erkennt schon wegen der Absenderangabe oder der Zitierung einschlägiger gesetzlicher Vorschriften über die Auskunftserteilung, daß dem Arbeitnehmer oder einem unterhaltsberechtigten Angehörigen Sozialleistungen gewährt werden. Die Zulässigkeit der Erfragung von Arbeitnehmerdaten wird daher durch das Erforderlichkeitsprinzip bestimmt. Wenn der Arbeitnehmer selbst die Nachweise über seine Einkünfte dem Sozialleistungsträger vorlegt, bleibt für die Anwendung der genannten Vorschriften kein Raum.

§ 1605 BGB hingegen, der insbesondere im Rahmen von Amtspflegschaften als Grundlage für die Beschaffung von Informationen über die Leistungsfähigkeit von Unterhaltspflichtigen herangezogen wird, gibt keine Auskunftsansprüche gegen den Arbeitgeber, sondern nur gegen die Unterhaltspflichtigen selbst. Diese haben allerdings über die Höhe der Einkünfte auf Verlangen Belege, insbesondere Bescheinigungen des Arbeitgebers vorzulegen.

Sicherlich ist es für Sozialleistungsträger oft bequemer, die erforderlichen Angaben beim Arbeitgeber unmittelbar zu erfragen, als den Pflichtigen selbst heranzuziehen. Es kommt deshalb immer wieder zu Beschwerden, in denen Betroffene völlig zu Recht beklagen, daß durch direkte Anfragen beim Arbeitgeber etwa der diskriminierende Eindruck erweckt wurde, sie kämen ihrer Unterhaltspflicht nicht nach.

Gelegentlich werden Anfragen an den Arbeitgeber nach dem Arbeitsverdienst auf § 1605 BGB gestützt und vom Arbeitgeber beantwortet, obwohl dieser erkennen müßte, daß diese Vorschrift nicht einschlägig ist.

Die Erfahrung, daß Arbeitgeber wohl ohne nähere Prüfung den Auskunftsersuchen von Sozialleistungsträgern entsprechen, machte sich die Bedienstete der Schulabteilung einer Kreisverwaltung in eigener Sache zunutze. Sie besorgte sich beim Jugendamt einen Vordruck „Anfrage über den Arbeitsverdienst", nannte als einschlägige Rechtsgrundlage § 1605 BGB und gelangte auf diese Weise schnell und direkt zu Angaben über die Unterhaltsfähigkeit ihres geschiedenen Ehemannes. Der LfD sieht in einem solchen Verhalten eine eklatante Dienstpflichtverletzung, konnte dem Betroffenen aber nur mitteilen, daß dienstordnungsrechtliche Maßnahmen oder eine strafrechtliche Würdigung außerhalb seiner Kompetenzen liegen. Der Landrat hat das Fehlverhalten der Bediensteten seiner Verwaltung eingeräumt und Ermahnungen ausgesprochen.

11.3.5 Archivierung von Akten

Das Inkrafttreten des Landesarchivgesetzes (LArchG) am 1. Januar 1991 beendete die Zeit der Rechtsunsicherheit bezüglich der Aufbewahrung und weiteren Verwendung archivwürdiger Materialien (vgl. Tz. 8.2). Dennoch verblieben insbesondere im Sozialleistungsbereich Unklarheiten. Diese beruhen zum einen auf einer undeutlichen Fassung der gesetzlichen Bestimmungen über die Anbietungspflicht, zum anderen auf der engen Verzahnung mit Bundesrecht, insbesondere auf der Konkurrenz des Landesarchivrechts mit bundesgesetzlichen Löschungs- oder Sperrungsvorschriften.

Die Zulässigkeit der Archivierung von Unterlagen eines Jugendamtes durch ein städtisches Archiv beurteilte der LfD wie folgt:

Nach § 2 Abs. 2 LArchG gewährleisten die kommunalen Gebietskörperschaften für ihre eigenen Archive, daß in ihnen hinsichtlich der Sicherung, Erhaltung und Nutzung des Archivgutes die für die staatlichen Archive geltenden Grundsätze beachtet werden. Diese Formulierung bedeutet, daß die Bestimmungen über die Anbietungspflicht (§ 7 LArchG) entsprechend anzu-

wenden sind. Nach § 7 Abs. 2 Nr. 1 LArchG sind auch solche Unterlagen anzubieten, die nach datenschutzrechtlichen Vorschriften vernichtet oder gelöscht werden müßten. Aufgrund der Verweisung auf § 1 Abs. 4 LArchG soll dies zwar nur für solche Unterlagen gelten, bezüglich deren eine durch landesrechtliche Vorschrift begründete Pflicht zur Vernichtung oder Löschung besteht (Sozialdaten sind aufgrund bundesrechtlicher Vorschriften – z. B. § 84 SGB X i. V. m. § 20 BDSG, § 64 KJHG – zu löschen). Dieser Gesetzeswortlaut, der im Verlauf der Ausschußberatungen im Blick auf einen konkreten Vorgang aus dem Anwendungsbereich des Landeskrankenhausgesetzes entstand, gibt indessen den gesetzgeberischen Willen nur unvollständig wieder. Gewollt war eine Ausnahme von der Löschungs- bzw. Vernichtungspflicht und eine Erstreckung der Anbietungspflicht auf alle Unterlagen, für die der Landesgesetzgeber regelungsbefugt ist, also auch auf solche Unterlagen, die durch das Sozialgeheimnis geschützt sind (entsprechend § 2 Abs. 4 Nr. 1 BArchG). Daß der Landesgesetzgeber befugt ist, derartige Regelungen zu treffen, steht außer Frage. § 71 Abs. 1 Satz 2 SGB X statuiert ausdrücklich eine Offenbarungsbefugnis für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut aufgrund gesetzlicher Vorschriften der Länder. Auch § 3 Abs. 3 Satz 4 LArchG, der eine Nutzung in Übereinstimmung mit § 5 Abs. 3 BArchG erst 80 Jahre nach der Entstehung zuläßt, deutet darauf hin, daß der Landesgesetzgeber eine Ausnahmeregelung – bezüglich der Löschung oder Vernichtung auch für den Anwendungsbereich des § 35 SGB I treffen wollte.

Für die Praxis ergibt sich hieraus folgendes: Der Sozialleistungsträger hat zu prüfen, ob die Löschungsvoraussetzungen nach allgemeinen oder speziellen sozialgesetzlichen Bestimmungen (beisp. § 84 SGB X, § 66 KJHG) vorliegen. Wenn dies der Fall ist, sind die Unterlagen dem Archiv anzubieten. Unterlagen sind zu löschen (beim Vorliegen der Voraussetzungen des § 66 Abs. 2 KJHG zu sperren), wenn das Archiv nicht innerhalb einer Frist von sechs Monaten erklärt, daß sie bleibenden Wert haben und deshalb übernommen werden (§ 8 Abs. 1 LArchG).

Es ist davon auszugehen, daß nur ein sehr geringer Teil der bei Sozialleistungsträgern entstehenden Vorgänge im Sinne dieser Vorschrift archivwürdig ist.

Die Nutzung von Archivgut bestimmt sich nach § 3 LArchivG. Für Materialien, die beispielsweise durch Sozialarbeiter an das Archiv abgegeben wurden, bestehen nach Absatz 5 dieser Vorschrift i. V. m. Absatz 2 Nr. 4 besondere Einschränkungen. § 203 Abs. 1 StGB, der die unbefugte Geheimnisoffenbarung durch Sozialarbeiter unter Strafe stellt, zwingt die Archivverwaltung, bei der Herausgabe von Unterlagen sorgfältig darauf zu achten, daß sie nur dem Mitarbeiter ausgehändigt werden, der im Sinne dieser Vorschrift befugt ist.

11.3.6 Offenbarung von Sozialdaten an Träger der freien Wohlfahrtspflege

Träger der freien Wohlfahrtspflege sind keine Sozialleistungsträger im Sinne des Sozialgesetzbuchs. Es bestehen zwar Regelungen über die Zusammenarbeit (z. B. § 28 Abs. 2 SGB I); im Rahmen der Offenbarung von Sozialdaten sind indessen die Träger der freien Wohlfahrtspflege grundsätzlich nicht privilegiert. Dies ist auch dann nicht der Fall, wenn ein Zusammenhang zwischen der jeweiligen Leistungsgewährung besteht, wie ihn das folgende Beispiel verdeutlicht:

Ein Caritasverband wollte von einem Sozialhilfeträger wissen, in welchen Fällen und in welcher Höhe Pflegegeldleistungen nach dem Bundessozialhilfegesetz und nach dem Landespflegegeldgesetz erbracht werden. Er benötigte diese Informationen als Grundlage für Entscheidungen über die Heranziehung von Personen, für die praktische Pflegeleistungen erbracht werden, zu angemessenen Kostenbeiträgen. In der Praxis – so wurde der DSK berichtet – komme es vor, daß die Sozialhilfeträger Pflegegeld zahlten, dies von den Empfängern aber bestritten werde, um von den Sozialstationen des Caritasverbandes eine weitgehend unentgeltliche Pflege zu erhalten.

Die DSK ging davon aus, daß es nicht zu den gesetzlichen Aufgaben des Sozialhilfeträgers im Sinne des § 69 Abs. 1 Nr. 1 SGB X gehört, dafür zu sorgen, daß ein freier Träger angemessene Kostenbeiträge erhält. Nur die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch könnte indessen eine Offenbarungsbefugnis begründen.

Obwohl die Anwendung der genannten Offenbarungsbestimmung nicht weiterführt, kann dem berechtigten Anliegen von freien Trägern jedoch in der Weise Rechnung getragen werden, daß die Empfänger von Pflegeleistungen um Einwilligung in die Offenbarung nach § 67 SGB X gebeten werden. Erteilen sie diese Einwilligung, besteht eine Offenbarungsbefugnis, erteilen sie die Einwilligung nicht, kann dies als Indiz dafür gewertet werden, daß eine für die Festsetzung der Kostenbeteiligung relevante Information zurückgehalten wird. Es wäre sicherlich nicht unbillig, in diesem Falle die höhere Kostenbeteiligung anzusetzen. Dies wäre im übrigen – sinngemäß – auch die Folge einer fehlenden Mitwirkung im Sozialleistungsverfahren nach § 66 SGB I.

11.3.7 Gewährung von Hilfe für Nichtseßhafte nach dem Bundessozialhilfegesetz

Aus dem kommunalen Bereich erhielt die DSK eine Anfrage zu folgendem Problem:

Aufgrund der geringen räumlichen Entfernung zwischen dem jeweiligen Sitz von Sozialhilfeträgern in Ballungsgebieten seien

Doppel- und Mehrfachzahlungen an Nichtseßhafte – Hilfe zum Lebensunterhalt nach dem Bundessozialhilfegesetz – an der Tagesordnung, weil diese im Laufe eines Tages mehrere Leistungsträger aufsuchten. Dies könne dadurch verhindert werden, daß die Betroffenen einen Ausweis erhielten, in dem der Empfang von Sozialhilfeleistungen bestätigt werde. Bei sorgfältiger Führung dieses Ausweises könne jeder Leistungsträger erkennen, wann und in welchem Umfange zuletzt Leistungen erbracht worden seien.

Die DSK wies darauf hin, daß dieses Verfahren sowohl unter dem Gesichtspunkt der Praktikabilität wie auch unter rechtlichen Gesichtspunkten bedenklich ist, denn es könnte nur dann zu den gewünschten Ergebnissen führen, wenn alle Nichtseßhaften mit einem solchen Ausweis ausgestattet würden, eine Mitführungs- und Vorlagepflicht bestünde und bei Nichtvorlage Sozialhilfeleistungen verweigert werden könnten. Die erforderliche Ausstattung mit Ausweisen erschien der DSK angesichts der Schwierigkeit, den Personenkreis der Nichtseßhaften innerhalb der Gesamtbevölkerung abzugrenzen und angesichts der Lebensgewohnheiten von Nichtseßhaften, völlig undurchführbar. Eine Ausweisvorlagepflicht stellt – datenschutzrechtlich betrachtet eine Verpflichtung zur Offenbarung von Daten, also einen Informationseingriff, dar. Dieser bedürfte einer detaillierten gesetzlichen Regelung. Unverzichtbar wäre bei zentraler Ausweiserteilung eine „Datei der Durchwanderer". Auch hierfür wäre eine gesetzliche Grundlage zu fordern. Die Sozialleistungsverweigerung bei Nichtvorlage des Ausweises wäre unvereinbar mit den im Bundessozialhilfegesetz normierten Anspruchsvoraussetzungen (Hilfebedürftigkeit), hätte also die Aufgabe eines tragenden Grundsatzes des Sozialleistungsrechts und – unter formalen Gesichtspunkten gesehen – eine Änderung des Bundessozialhilfegesetzes zur Voraussetzung.

Als rechtliche Grundlage einer Problemlösung kann nur der Untersuchungsgrundsatz des § 20 SGB X dienen. Danach ermittelt die Behörde den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen und ist dabei an das Vorbringen und die Beweisanträge der Beteiligten nicht gebunden. Hieraus folgt die Befugnis der Sozialämter, in Fällen, in denen die mißbräuchliche Inanspruchnahme von Sozialleistungen vermutet wird, nähere Erkundigungen einzuziehen, m. a. W., bei anderen Sozialleistungsträgern anzufragen (auch telefonisch), ob und ggf. für welchen Zeitraum einer bestimmten Person Sozialleistungen gewährt wurden.

Eine Offenbarungsbefugnis sowohl für die anfragende wie auch für die im Rahmen der Amtshilfe in Anspruch genommene Behörde ergibt sich aus § 69 Abs. 1 Nr. 1 SGB X, denn es ist eine gesetzliche Aufgabe von Sozialleistungsträgern, den Doppelbezug oder andere Formen unberechtigter Inanspruchnahme von Leistungen zu verhindern.

Es ist einzuräumen, daß diese Vorgehensweise in der Wirkung anderen, institutionalisierten Formen der Überwachung – etwa durch ein Ausweissystem, durch Warnlisten oder durch eine „Leistungsdatenbank" mit Zugriffsmöglichkeiten für Sozialleistungsträger eines bestimmten Bereichs – nicht entsprechen mag. Die bestehenden gesetzlichen Regelungen lassen indessen – und keineswegs nur aus datenschutzrechtlichen Gründen – für diese Überwachungsformen keinen Raum.

11.3.8 Offenbarung von Sozialdaten an den Rechnungsprüfungsausschuß eines Landkreises

Eine Kreisverwaltung fragte an, ob und ggf. unter welchen Voraussetzungen dem Rechnungsprüfungsausschuß und dem Kreistag – zur Behandlung in nichtöffentlicher Sitzung – Auskünfte über den Inhalt von Akten des Jugendamtes erteilt werden dürften. Die DSK nahm wie folgt Stellung:

Nach § 50 Nr. 6 LKO i. V. m. § 110 Abs. 1 und § 112 Abs. 1 GemO hat der Rechnungsprüfungsausschuß die Aufgabe, die Jahresrechnung des Landkreises mit allen Unterlagen zu prüfen. Im Grundsatz hat der Rechnungsprüfungsausschuß einen Auskunftsanspruch und kann Aktenvorlage verlangen.

Zugleich ist der Rechnungsprüfungsausschuß als Rechnungsprüfungs„behörde" Normadressat des § 35 SGB I und hat demzufolge das Sozialgeheimnis zu beachten. Anders als beispielsweise der Jugendwohlfahrtsausschuß, der Sozialausschuß oder der Kreisrechtsausschuß hat er aber keine originären Entscheidungszuständigkeiten in Sozialangelegenheiten; er ist also kein Sozialleistungsträger und bildet auch im funktionalen Sinne keine Einheit mit einem Sozialleistungsträger. Hieraus folgt, daß die Weitergabe von Informationen durch den Sozialleistungsträger Jugendamt an den Rechnungsprüfungsausschuß eine Offenbarung i. S. der §§ 35 SGB I, 67 ff. SGB X darstellt.

Nach § 69 Abs. 1 Nr. 1 SGB X ist diese Offenbarung zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch eine in § 35 SGB I genannte Stelle erforderlich ist. Die Ermöglichung der Rechnungsprüfung ist eine gesetzliche Aufgabe des Jugendamtes; daß auch der Gesetzgeber dieser Ansicht war, ergibt sich schon daraus, daß er die Rechnungsprüfungsbehörden in den Kreis der Normadressaten des § 35 SGB I einbezogen hat. Im Grundsatz liegen also die Offenbarungsvoraussetzungen vor. Inhaltlich begrenzt werden sie aber durch das Erforderlichkeitsprinzip.

Eine Offenbarung von Sozialdaten an den Rechnungsprüfungsausschuß kommt also nur insoweit in Betracht, als die zu übermittelnden Informationen für Zwecke der Rechnungsprüfung erforderlich sind.

Da die Offenbarung von Sozialdaten als Grundrechtseingriff zu qualifizieren ist, ist es Sache der diesen Eingriff vornehmenden Stelle, also des um Offenbarung ersuchten Leistungsträgers, das Vorliegen der Voraussetzungen einer Offenbarungsbefugnis zu prüfen. Als erstes ist die Frage zu stellen, ob die Offenbarung überhaupt Prüfungszwecken dient. Der Rechnungsprüfungsausschuß ist verpflichtet, die Gründe für das Offenbarungsersuchen gegenüber dem Sozialleistungsträger darzulegen.

Ferner ist bei der Prüfung des zulässigen Umfanges einer Offenbarung der Verhältnismäßigkeitsgrundsatz zu beachten. Danach müssen die zu offenbarenden Informationen für die Erfüllung der Prüfungsaufgabe auch geeignet sein. Hieraus ergeben sich ebenfalls Beschränkungen, die es ausschließen, daß dem Rechnungsprüfungsausschuß Akten oder Auszüge aus Akten zur Verfügung gestellt werden, die nicht unmittelbar für die Wahrnehmung seiner Aufgaben nach § 112 Abs. 1 GO relevant sind. Bei Akten des Sozialdienstes oder bei Pflegschaftsakten sind grundsätzlich Zweifel angezeigt.

Die Unterrichtungsrechte des Kreistages ergeben sich aus § 26 LKO. Sie sind inhaltlich begrenzt und lassen es in Verbindung mit den Offenbarungsbestimmungen des Sozialgesetzbuchs nach Auffassung der DSK nicht zu, daß in öffentlicher oder nichtöffentlicher Kreistagssitzung personenbeziehbare Auskünfte in Sozialleistungsangelegenheiten erteilt werden.

11.3.9 „Vaterschaft im Abfalleimer"

Unter dieser Schlagzeile und ähnlichen Überschriften berichteten mehrere Tageszeitungen, Wochenblätter und Magazine über Fundstücke, die beim Durchsuchen der Abfallcontainer einzelner Behörden zutage gefördert wurden. Hierzu gehörten handschriftliche Vermerke, ausgefüllte Vordrucke und Entwürfe von Briefen, die zum Teil unverändert, zum Teil aber auch zerknüllt oder zerrissen in der Weise entsorgt worden waren, daß sie zuerst in den Papierkorb und dann in außerhalb der Verwaltungsgebäude aufgestellte Abfallcontainer geworfen wurden. Die Rekonstruktion zerrissener Materialien war in keinem Falle besonders schwierig, denn nur sehr selten wurde das Format DIN A 6, das beim zweimaligen Zerreißen eines DIN A 4 – Blattes entsteht, unterschritten. Zu den Fundstücken gehörte beispielsweise ein wegen mehrerer Schreibfehler nicht abgesandter Brief eines Jugendamtes an ein Familiengericht. Das Schreiben enthielt die Namen und Geburtsdaten der betroffenen Kinder und informierte über die familiäre Situation. Aus der Zusammenfassung eines Gesprächs, das der Vater im Jugendamt geführt hatte, war zu entnehmen, warum er seine Ehefrau nicht gerne in der Rolle der Alleinerziehenden sehen wollte. Daß diese vom Vater genannten Gründe für die betroffene Frau nicht sehr schmeichelhaft, aus der Sicht des Datenschutzes jedenfalls außerordentlich sensitiv waren, bedarf kaum einer Erwähnung. Ein noch brisanteres Schriftstück aus den Mülltonnenfunden betraf eine Vaterschaftsanerkennung. Adressiert war der Brief an einen Mann, der als Vater in Frage kam. Zugleich wurde aber auch eingeräumt, daß ein anderer namentlich benannter Mann als Erzeuger des Kindes in Betracht kommen könne.

In den Mülltonnen eines Gesundheitsamtes wurden komplette Untersuchungsberichte mit Namensangaben und Gesundheitszeugnisse gefunden.

Ein Arbeitsamt hatte Zahlungslisten mit den Namen und Anschriften von Arbeitslosen in Müllcontainern entsorgt.

Die DSK hat in den bekannt gewordenen Fällen, soweit sie zuständig war, Beanstandungen wegen Verletzung von Datenschutzvorschriften ausgesprochen, in den anderen Fällen die zuständige Aufsichtsbehörde informiert. Ihren Forderungen, Schriftgut und Aktenvernichtungsgeräte zum Zwecke der geordneten Entsorgung anzuschaffen, wurde – im Blick auf das entstandene öffentliche Aufsehen – ganz besonders schnell entsprochen.

Die öffentliche Berichterstattung hat sicherlich bei vielen Behörden zu einer Sensibilisierung und vielleicht auch zu konkreten Maßnahmen geführt. Ein Problem scheint indessen zu sein, daß die geordnete Entsorgung von Schriftgut nach einem heilsamen Schock, wie er von der Medienberichterstattung sicherlich ausging, allmählich wieder einer gewissen Sorglosigkeit zum Opfer fällt. Hiervor kann nur gewarnt werden, denn zum einen ist es außerordentlich leicht, eine Verwaltung, die in dieser Hinsicht Fehler macht, öffentlich zu denunzieren, zum anderen haben die Verantwortlichen dienstrechtliche Maßnahmen zu gewärtigen. Entscheidend ist freilich die Beurteilung aus der Sicht des Betroffenen: Er muß aufgrund gesetzlicher Verpflichtung oder zur Erlangung staatlicher Hilfen seine Daten preisgeben und hat deshalb einen Anspruch darauf, daß der Schutz dieser Informationen sichergestellt wird.

11.4 Heimaufsicht

11.4.1 Pflegedokumentation

Eine Bezirksregierung verlangte als Heimaufsichtsbehörde von den Trägern der Alten- und Pflegeheime ihres Zuständigkeitsbereichs, daß sie für jeden Heiminsassen, der sich in ärztlicher Behandlung befindet, die Diagnose und Medikation in einer „Pflegedokumentation" nachweisen. Demgegenüber vertraten die behandelnden Ärzte die Auffassung, daß keineswegs in allen Fällen ein Erfordernis besteht, die Heimleitung zum Zwecke der Führung einer Pflegedokumentation zu unterrichten. Eine Kassenärztliche Vereinigung erbat eine Stellungnahme der DSK.

Diese wies darauf hin, daß die Frage, ob und in welchem Umfange Patientendaten zu Dokumentationszwecken offenbart werden dürfen, nach der Ärztlichen Berufsordnung zu beurteilen ist. Nach § 2 Abs. 1 hat der Arzt über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Nach Absatz 4 der Vorschrift ist der Arzt, soweit er von der Schweigepflicht entbunden worden ist oder der Schutz eines höheren Rechtsgutes dies erfordert, zur Offenbarung befugt, aber – vorbehaltlich besonderer gesetzliche Bestimmungen – nicht verpflichtet. Hieraus folgt, daß die Entscheidung, ob und in welchem Umfange personenbezogene medizinische Informationen zum Zwecke der Aufnahme in die Pflegedokumentation an Bedienstete von Alten- und Pflegeheimen oder an die Heimleitung weitergegeben werden, vom Arzt unter Berücksichtigung des Selbstbestimmungsrechts des Patienten zu treffen ist. Liegt eine Schweigepflichtsentbindung des Patienten vor, kann er die Diagnose offenbaren, ohne hierzu verpflichtet zu sein. Fälle, in denen ein Arzt etwa gegen den Willen (bzw. trotz Zustimmung) des Patienten eine Diagnose nicht offenbart, finden ihre Lösung dadurch, daß der Arzt gegenüber dem Patienten auskunftspflichtig ist und dieser die Diagnose selbst weitergeben kann.

Schwieriger sind solche Fälle zu beurteilen, in denen Patienten vorübergehend oder dauernd außerstande sind, eine Willensentscheidung zu treffen bzw. eine rechtsgültige Einwilligungserklärung zu erteilen. In derartigen Fällen ist als Rechtfertigungsgrund für eine Offenbarung von Patientendaten in erster Linie die mutmaßliche Einwilligung von Bedeutung. Es kommt in diesem Zusammenhang ganz wesentlich darauf an, daß die Offenbarung im Interesse des Patienten geboten ist. Ein etwa bestehendes Interesse der Heimleitung oder Heimaufsicht, eine Pflegedokumentation zu vervollständigen, dürfte nicht ausreichen. Die Offenbarung muß patientendienlich sein, mit anderen Worten, die Kenntnis der Diagnose muß für die Ausübung einer sachgerechten Pflege von Bedeutung sein. Soweit die Berufsordnung eine Offenbarung zum Schutze eines höheren Rechtsgutes zuläßt, kommen insbesondsere gesetzliche Offenbarungsbefugnisse oder Mitteilungspflichten in Betracht (z. B. nach dem Bundesseuchengesetz), ferner die Offenbarung aufgrund rechtfertigenden Notstandes oder aufgrund Garantenstellung.

11.4.2 Überwachung des Briefverkehrs

Im Zusammenhang mit der Bearbeitung einer Eingabe erhielt die DSK Kenntnis vom Inhalt einer Vollmacht, wie sie vereinzelt in Behindertenseinrichtungen als Ergänzung zum Heimvertrag Verwendung findet. Danach erteilt der Vormund/Pfleger eines Behinderten der Heimleitung die Vollmacht, „im erforderlichen Umfang Einsicht in die Korrespondenz zu nehmen". Die DSK äußerte Bedenken bezüglich der Befugnis des Personensorgeberechtigten, eine derart weitgehende Ermächtigung auf die Heimleitung zu übertragen.

Die Heimaufsichtsbehörde teilte diese Bedenken und sorgte für die Änderung des Erklärungstextes und des Verfahrens.

11.4.3 Beratung von Pflegekräften durch Psychologen

In der Diskussion war auch die Frage, ob es zulässig ist, im Rahmen der Beratung von Mitarbeitern eines Heims für geistig Behinderte durch einen Psychologen Einzelfälle aus dem jeweiligen Arbeitsbereich des Mitarbeiters zu besprechen (Falldarstellung, Darstellung der bisherigen Entwicklung des Behinderten, Erarbeitung eines Betreuungs-Förderkonzeptes).

Die DSK vertrat die Auffassung, daß die Erörterung von Einzelfällen der Betreuungspraxis nur mit Zustimmung des Behinderten zulässig ist. Für diese Zustimmung kommt es nicht auf die Geschäftsfähigkeit des Heiminsassen an; entscheidend ist, ob er über die notwendige Einsicht in die Bedeutung und Tragweite des Geschehens verfügt. Nur wenn dies nicht der Fall ist, kann seine Zustimmung durch die Zustimmung des Sorgeberechtigten ersetzt werden. Für die Erklärung der Einwilligung besteht kein Formerfordernis. Grundsätzlich sind auch konkludente oder mutmaßliche Einwilligungen zugelassen. Wegen möglicher Nachweisprobleme ist eine Heimleitung aber gut beraten, wenn sie auf Schriftform besteht. Wird die Zustimmung nicht erteilt, ist eine Erörterung von Einzelfällen nur in anonymer Form zulässig.

12 Ausländer und Vertriebene

12.1 Entwurf eines Ausländerzentralregistergesetzes

Das Ausländerzentralregister besteht seit dem Jahre 1953 als bundeszentrale Kartei und wird seit 1967 in einem automatisierten Verfahren geführt. Im Gesetz über die Errichtung des Bundesverwaltungsamtes vom 28. Dezember 1959 (BGBl. I S. 829) wurde dessen Zuständigkeit für das Register begründet (§ 6). Regelungen über die Aufgaben und die nähere Ausgestaltung des Registers sowie über die Kommunikation mit anderen Stellen sind in der Allgemeinen Verwaltungsvorschrift zur Ausführung des Ausländergesetzes vom 7. Juli 1967 (GMBl. S. 231) i. d. F. der Bekanntmachung vom 10. Mai 1977 (GMBl. S. 202), geändert durch die Allgemeine Verwaltungsvorschrift vom 7. Juli 1978 (GMBl. S. 368), sowie in Rundschreiben und Erlassen des Bundesministers des Innern enthalten.

Seit Jahren wird aus der Sicht des Datenschutzes für dieses Register die notwendige gesetzliche Grundlage gefordert. Nunmehr liegt ein Arbeitspapier „Entwurf eines Bundeszentralregistergesetzes" als Referentenentwurf aus dem Bundesministerium des Innern vor, der dem LfD vom Ministerium des Innern und für Sport zugeleitet wurde. Zu dem Entwurf wurde wie folgt Stellung genommen:

Die durch den Entwurf eröffneten Verwendungsmöglichkeiten des Registers gehen über einen bloßen Identitäts-, Aufenthalts- und Aktennachweis weit hinaus, indem wesentliche materielle Informationen über die Person eines Ausländers in das Register eingespeichert und diesem entnommen werden können. Damit entsteht die Gefahr, daß der grundsätzlich gebotene Rückgriff auf die jeweiligen Sachakten unterbleibt. Die zwangsläufig verkürzte – und oft auch aus dem Zusammenhang gerissene Darstellung im Register könnte dann ohne Kenntnis des nur aus den Akten ersichtlichen Kontextes zur Entscheidungsgrundlage gemacht werden, womit erhebliche Risiken für den Betroffenen verbunden sind.

Ein weiterer Gefährdungspunkt ist die Vielzahl der Fachbehörden, die Daten übermitteln sollen oder empfangen können. Dies ist im Zusammenhang mit der umfassenden Einrichtung von dialogfähigen Online-Anschlüssen zu sehen. Direktanschlüsse sind aus der Sicht des Datenschutzes u. a. deshalb problematisch, weil sie eine vorherige Kontrolle der Berechtigung des einzelnen Abrufs ausschließen. Die geschilderte Konzeption führt dazu, daß über den einzelnen Ausländer aus unterschiedlichen Bereichen zum Teil sehr sensible Daten zusammengeführt werden, die auch ohne entsprechende Aufbereitung ein aufschlußreiches Persönlichkeitsbild ermöglichen.

Vor diesem Hintergrund sind folgende Punkte hervorzuheben :

- Die oben beschriebene Substitutionsfunktion des Registers greift mit der Zulassung der Speicherung verkürzter Sachverhalte aus den verschiedensten Lebensbereichen besonders in das Recht auf informationelle Selbstbestimmung ein und bedarf daher einer entsprechend normenklaren gesetzlichen Regelung. Der in § 2 (Zwecke des Registers) Abs. 1 Ziff. 3 enthaltene lapidare Hinweis auf „andere Sachverhalte" reicht da ebensowenig aus wie die schlichte Nennung nicht näher beschriebener „Sachverhalte" in § 3 (Anlaß der Speicherung und Inhalt des Registers) Abs. 3 Ziff. 4.

- Nach § 3 Abs. 2, Ziff. 3 werden Bedenken gegen die Einreise eines Ausländers gespeichert, die bestehen, wenn Tatsachen vorliegen, die nach § 7 Abs. 2 des Ausländergesetzes die Versagung der Aufenthaltsgenehmigung begründen. Die Aufzählung der Versagungsgründe reicht von der mangelnden Fähigkeit zum Bestreiten des Lebensunterhaltes bis zu „sonstigen Gründen", aus denen der Aufenthalt des Ausländers die Interessen der Bundesrepublik Deutschland beeinträchtigt oder gefährdet. Außerdem können die umfangreichen in § 46 AuslG aufgezählten Ausweisungsgründe hinzugezogen werden.

  Wenn alle diese Fallgruppen zu verkürzten Sachverhaltsspeicherungen führen sollen, dann ist ein Höchstmaß an rechtsstaatlichen Sicherungen geboten. Vor einer abschließenden Beurteilung sollte daher dargelegt werden, welche konkreten Vorstellungen hinsichtlich der Art und des Inhalts der Speicherung von „Sachverhalten" in der Praxis bestehen. Jedenfalls ist ein unmittelbarer Bezug auf die gesetzliche Fallgruppe unerläßlich, ebenso wie die Speicherung eines bloßen Verdachts ausgeschlossen sein muß. Auf jeden Fall ist bereits im Gesetzestext als Speicherungsvoraussetzung das Vorliegen bestimmter Tatsachen zu fordern. Außerdem ist vorzusehen, daß die die Daten anliefernden bzw. einspeichernden Stellen durch fachspezifische Verwaltungsvorschriften an bestimmte einengende Speicherkriterien gebunden werden, die es auch der Registerbehörde erlauben, die Rechtmäßigkeit der Speicherung wenigstens hinsichtlich ihrer Plausibilität (§ 6 Abs. 1 Ziff. 5) zu überprüfen.

- Es sind einengende Regelungen bei der Sachverhaltsspeicherung in Sozialleistungsfällen nach § 3 Abs. 2 Ziff. 3 des Entwurfs i. V. m. § 7 Abs. 2 Ziff. 1 und § 46 Ziff. 6 und 7 AuslG zu fordern. Dabei handelt es sich im wesentlichen um die Inanspruchnahme von Sozialhilfe nach dem BSHG sowie Hilfe zur Erziehung außerhalb der eigenen Familie oder Hilfe für junge Volljährige nach dem KJHG (SGB VIII). Hier ist bereits unklar, ob – wie der Text des Ausländergesetzes vermuten ließe – alle Arten von Erziehungshilfen gemeint sind oder nur bestimmte. In offiziellen Anwendungshinweisen zu § 76 Abs. 2 des Ausländergesetzes sind verschiedene Sachverhalte von der Unterrichtung an die Ausländerbehörde ausgenommen, so Sozialhilfeleistungen, die aufgrund gesetzlicher Vorschriften vorläufig für einen anderen Leistungsträger (z. B. für die Bundesanstalt für Arbeit) oder an Ausländer mit Aufenthaltsgenehmigung (nicht Visum) zur Behebung einer nur vorübergehenden Notlage für die Dauer von höchstens sechs Monaten erbracht werden. Hierzu zählen auch Hilfen in besonderen Lebenslagen (§§ 27 – 75 BSHG), wenn es sich um keine Dauerleistung handelt oder wenn die Summe der Hilfen DM 10 000,– nicht übersteigt. Das gleiche gilt für bestimmte Hilfeleistungen an junge Volljährige nach Maßgabe des KJHG (SGB VIII) bei Nachweis einer Aufenthaltsberechtigung oder einer unbefristeten Aufenthaltserlaubnis.

Der LfD hält es nicht für erforderlich, im Ausländerzentralregister Daten zu speichern, die in der Verwaltungspraxis nach dem Ausländergesetz jedenfalls weitgehend nicht an die Ausländerbehörden zu übermitteln sind. Es sollten deshalb entsprechende Abgrenzungen entweder in der Speicherungsnorm des § 3 Abs. 2 Ziff. 3 des AZRG oder (mittels Artikelgesetz) im Ausländergesetz in geeigneter Weise vorgenommen werden.

- Gemäß § 4 kann ein Betroffener verlangen, daß eine Auskunfts- und Übermittlungssperre u. a. in bezug auf ausländische Behörden gespeichert wird. „Bei überwiegendem öffentlichen Interesse" kann aber doch übermittelt werden. Der Betroffene ist zwar zuvor zu hören; auch dies kann unterbleiben, wenn es dem Auskunftszweck zuwiderläuft. Angesichts der totalitären Regierungsform in einer Vielzahl ausländischer Staaten erscheint die beabsichtigte Regelung in dieser Form bedenklich. Es muß auf jeden Fall vermieden werden, daß durch Übermittlungen an ausländische Stellen insbesondere totalitärer Staaten Personen gefährdet werden, seien es Angehörige des Betroffenen oder er selbst bei einer späteren Einreise in seinen Heimatstaat. Ein „überwiegendes öffentliches Interesse" kann daher nur in schwerwiegenden Fällen genügen, die nach Möglichkeit im Gesetz als Fallgruppen aufgelistet werden müßten. Besonders enge Voraussetzungen sind dann vorzusehen, wenn die vorherige Anhörung des Betroffenen unterbleibt.

- Die Einrichtung des Direktabrufverfahrens für die Verfassungsschutzbehörden und den Bundesnachrichtendienst wird in der vorgesehenen amtlichen Begründung (S.29) damit gerechtfertigt, daß dies „auch" der „Wahrung der besonderen Vertraulichkeit ihrer Aufgabenerfüllung" diene. Dies stellt keinen spezifisch das Ausländerregister betreffenden Gesichtspunkt dar. Hier sollte zumindest eine ergänzende Begründung erfolgen, die insbesondere auf die Zahl und die Dringlichkeit der zu erwartenden Abrufe abzustellen hätte.

12.2 Mitteilungen an die Ausländerbehörden bei Ablehnung von Personen als Aussiedler oder Vertriebene

Durch die Anfrage einer Stadtverwaltung wurde der LfD auf die fehlende Übermittlungsgrundlage für bestimmte notwendige Mitteilungen der Vertriebenenbehörden an die Ausländerbehörden aufmerksam. Obwohl nach dem Aussiedleraufnahmegesetz (AAG) vom 28. Juni 1990 der Antrag auf Anerkennung als Deutscher i. S. von Art. 116 GG bzw. auf Erteilung eines Vertriebenenausweises bereits aus dem Herkunftsland an das Bundesverwaltungsamt gestellt werden muß, ergehen nach Einreise in das Bundesgebiet mitunter Ablehnungsbescheide. Das geschieht insbesondere dann, wenn sich trotz der bereits durch deutsche Stellen im Herkunftsland durchgeführten Plausibilitätsprüfung ergibt, daß die Anerkennungsvoraussetzungen im einzelnen Fall doch nicht vorliegen. Für die Dauer des Verfahrens wird der Antragsteller vorläufig wie ein Deutscher im Sinne des Art. 116 Abs. 1 GG behandelt. Spätestens mit der Wirksamkeit des Ablehnungsbescheides hat er jedoch wieder ausschließlich den Status eines Ausländers, der sich nunmehr ohne Legitimierung nach dem Ausländergesetz in der Bundesrepublik aufhält. Die zuständige Ausländerbehörde hat die Aufgabe und die Verpflichtung, ihn zum alsbaldigen Verlassen des Bundesgebietes zu veranlassen, wozu sie jedoch Kenntnis von der Tatsache der Ablehnung haben muß. Eine regelmäßige Übermittlung durch die Vertriebenenbehörde an die Ausländerbehörde in diesen Fällen ist jedoch weder im Bundesvertriebenengesetz noch in der Ausländerdatenmeldeverordnung vorgesehen. Die Notwendigkeit eines unverzüglichen Tätigwerdens der Ausländerbehörde ist aber unbestritten. So war in Erfahrung zu bringen, daß die Absicht besteht, in dem im Entwurf vorliegenden Gesetz zur Bereinigung von Kriegsfolgengesetzen im Falle der Ablehnung von entsprechenden Anträgen eine Unterrichtung durch die Vertriebenenbehörden an alle Stellen vorzusehen, die dem Antragsteller Rechte einräumen. Hierunter würden dann auch die Ausländerbehörden fallen.

Zumindest bis zum Zeitpunkt der Novellierung bestehen keine Einwände, wenn die Vertriebenenbehörden die Ausländerbehörden nach § 76 Abs. 2 Ziff. 1 jeweils von der Ablehnung unterrichten. Nach dieser Vorschrift haben alle öffentlichen Stellen die Ausländerbehörde unverzüglich zu unterrichten, wenn sie von dem Aufenthalt eines Ausländers Kenntnis erhalten, der weder eine erforderliche Aufenthaltsgenehmigung noch eine Duldung besitzt. Hiervon wird die Vertriebenenbehörde nach Lage der Dinge im Regelfall ausgehen können, wenn der Antrag abgelehnt worden ist. Man wird von ihr nicht fordern können, sich zuvor zu versichern, ob der abgelehnte Antragsteller nicht zwischenzeitlich in anderem Zusammenhang eine Aufenthaltsgenehmigung erhalten hat.

Bei der Unterrichtung der Ausländerbehörde ist jedoch die Mitteilung auf die Angaben zur Person entsprechend der Auflistung in § 1 Abs. 2 Nr. 1 bis 6 AuslDÜV sowie auf die Mitteilung des Verlustes der vorläufigen Rechtsstellung als Deutscher zu beschränken. Keinesfalls ist der komplette Ablehnungsbescheid zu übersenden.

Gleichwohl ist zu fordern, daß auch für die geschilderte Fallgruppe baldmöglichst eine ausdrückliche und für den Bürger transparente spezifische rechtliche Grundlage geschaffen wird.

12.3 Erkennungsdienstliche Behandlung von Asylbewerbern

Identifizierungsmaßnahmen anhand daktyloskopischer Spuren verlaufen nach einer in Richtlinien geregelten Arbeitsteilung zwischen Bund und Ländern. Dazu besteht neben den konventionellen Sammlungen ein automatisiertes Bund-Länder-System für Fingerabdruckblätter. Auswertung und Speicherung erfolgen gemäß BKA-Gesetz beim Bundeskriminalamt als zentraler Sammelstelle. Die technische Leistungsfähigkeit des gegenwärtigen Systems, die ohnehin ihre Grenze erreicht hat, wird nunmehr vollkommen überfordert durch die Eingliederung der Unterlagen der Polizeien der neuen Bundesländer sowie der verstärkten Erfassung von Fingerabdruckblättern von Asylbewerbern. Da die Polizei auf ein leistungsfähiges Auswertungssystem angewiesen ist, hat die Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (AG Kripo) dem

Arbeitskreis II „Öffentliche Sicherheit und Ordnung" der Innenministerkonferenz vorgeschlagen, das „Automatisierte Fingerabdruckidentifizierungssystem – AFIS –" ab 1993 einzuführen. Vorbehaltlich der Zustimmung der Finanzminister für die Beschaffungsmaßnahme hat die Innenministerkonferenz den Vorschlag gebilligt. Gleichzeitig wurde beschlossen, möglichst alle Asylantragsteller erkennungsdienstlich zu behandeln. Diese Daten sollen zur Feststellung der Identität in AFIS mitgespeichert werden, dürfen allerdings nicht für andere Zwecke verwendet und nicht mit anderen erkennungsdienstlichen Unterlagen zusammengeführt werden. Nach § 13 Abs. 3 Satz 1 des Asylverfahrensgesetzes leistet das Bundeskriminalamt dem Bundesamt für die Anerkennung ausländischer Flüchtlinge Amtshilfe bei der Auswertung der gewonnenen erkennungsdienstlichen Unterlagen.

Nachdem in den letzten Jahren eine deutliche Zunahme der Fälle zu verzeichnen ist, in denen Wiederholungsanträge mißbräuchlich unter veränderter Identität mit Hilfe gefälschter Papiere gestellt wurden, ist die Praxis dazu übergegangen, Zweifel an der Identität von Asylbewerbern regelmäßig dann anzunehmen, wenn sie aus Ländern kommen, in denen erfahrungsgemäß häufig gefälschte Identitätspapiere illegal beschafft werden können oder in denen es möglich ist, legal und ohne besondere Schwierigkeiten die Identität zu wechseln. Die Quote der ED-Behandlungen von Asylbewerbern stieg auf diese Weise im vergangenen Jahr auf etwa 30 v. H. Vor diesem Hintergrund beabsichtigt die Konferenz der Innenminister, die Quote der erkennungsdienstlich zu behandelnden Asylsuchenden zu erhöhen und möglichst alle Antragsteller einzubeziehen.

Bei der erkennungsdienstlichen Behandlung handelt es sich um einen Eingriff in das Grundrecht auf körperliche Unversehrtheit, das auch Ausländern zusteht. Die erforderliche gesetzliche Eingriffsermächtigung bietet § 13 des Asylverfahrensgesetzes, wonach die Identität des Asylbewerbers durch erkennungsdienstliche Maßnahmen zu sichern ist, wenn sie nicht eindeutig bekannt ist. Damit wird zunächst zwingend vorgeschrieben, daß erkennungsdienstliche Maßnahmen nur nach entsprechenden Prüfungen in einzelnen Fällen vorgenommen werden können, was sich aus dem Wortlaut und der Struktur der Norm ebenso ergibt wie aus ihrem Charakter als Eingriffsbefugnis gegenüber einem besonders geschützten Rechtsgut. Dies wird auch im Ministerium des Innern und für Sport nicht anders gesehen. Einer entgegenstehenden Auffassung der Innenministerkonferenz ist daher aus Datenschutzgründen entschieden zu widersprechen.

Schwieriger stellt sich demgegenüber die Beurteilung der auch in Rheinland-Pfalz geübten Praxis dar, Asylantragsteller aus bestimmten Staaten, in denen die Identität ihrer Bürger in großzügiger Weise gestaltbar ist, generell erkennungsdienstlich zu behandeln. Die Praxis geht davon aus, daß grundsätzlich die Personalpapiere aus solchen Staaten nicht ohne besondere Prüfung als eindeutige Identitätsnachweise angesehen werden können, was insoweit zur weitgehenden ID-Behandlung der Betroffenen führt. § 13 Asylverfahrensgesetz setzt – anders als § 41 des Ausländergesetzes – nicht voraus, daß Zweifel an der Identität bestehen. Er bestimmt vielmehr, daß die Identität durch ED-Maßnahmen gesichert wird, wenn sie nicht eindeutig bekannt ist. Der legislative Zweck der Vorschrift besteht darin, für die Zukunft zu sichern, daß nicht mit einer anderen Identität erneut von derselben Person ein Asylantrag gestellt wird. So ist auch die immerhin zehnjährige Aufbewahrungsfrist in Absatz 2 zu verstehen. Der eindeutige Normzweck ist bei Asylbewerbern aus Ländern mit einem verhältnismäßig hohen Aufkommen an unzutreffenden Personalpapieren auf andere Weise nicht zu erreichen. Dabei kann nicht unberücksichtigt bleiben, daß § 13 Abs. 1 Asylverfahrensgesetz nicht nur eine Eingriffsbefugnis enthält, sondern – wie die Formulierung „...ist ... zu sichern" erkennen läßt, ein Gebot zum Handeln. Auch die sonst kritische Kommentierung bei Kanein (Kommentar zum Ausländerrecht, 4. Aufl., München 1988, Bem. 1 zu § 13 AsylVfG) räumt, gestützt auf die amtliche Begründung, die Tendenz des Gesetzgebers ein, „in möglichst großem Umfang von erkennungsdienstlichen Maßnahmen Gebrauch zu machen".

Nach diesen Überlegungen scheint es nicht gerechtfertigt, die beschriebene Praxis der Behörden in Asylverfahren für unzulässig zu erklären, solange sie sich auf Asylbewerber aus solchen Staaten beschränkt, bei denen tatsächlich die beschriebenen Möglichkeiten in nennenswertem Umfang bestehen und genutzt werden. Wann und wo dies der Fall ist, sollte – um die Praxis möglichst transparent zu halten – in Verwaltungsvorschriften festgelegt werden, auch wenn die Notwendigkeit besteht, diese regelmäßig den neuesten Erkenntnissen anzupassen. Dabei ist auch zu bestimmen, daß Asylbewerber, deren Identität auf andere Weise feststellbar ist – etwa mit Hilfe anderer Dokumente oder aufgrund persönlicher Bekanntheit –, nicht erkennungsdienstlich behandelt werden.

Soweit die Auswertungsergebnisse beim BKA gespeichert werden, begegnet dieser Umstand keinen Bedenken, weil § 13 Abs. 3 Satz 2 Asylverfahrensgesetz offensichtlich hiervon ausgeht, indem die Löschungsregeln des Absatzes 2 für das BKA ausdrücklich für anwendbar erklärt werden. Ob die in Satz 3 weiter vorgesehene Nutzung im Rahmen der Strafverfolgung und der Gefahrenabwehr allerdings einen Direktzugriff für alle Polizeibehörden rechtfertigt, bedarf der eingehenden Prüfung. Dies muß insbesondere wegen der damit verbundenen Stigmatisierung für eine Einstellung der Daten in das INPOL-System gelten. Das sollte bei AFIS nach Möglichkeit vermieden werden.

Da die ED-Daten von Asylbewerbern nach ihrer gesetzlichen Zweckbestimmung der Identitätssicherung im Asylverfahren dienen – die fallweise zugelassene Mitnutzung für repressive und präventive Zwecke (Gefahrenabwehr) ändert hieran nichts – ist bei der Prüfung, ob Abdrücke von allen zehn Fingern abgenommen werden müssen, ein sehr strenger Maßstab anzulegen. Wenn es zutrifft, daß zur Identitätssicherung der Abdruck und die Verformung des rechten Zeigefingers ausreichen, wäre es unverhältnismäßig und damit rechtswidrig, darüber hinauszugehen.

12.4 Zwangsweise ärztliche Untersuchung von Asylbewerbern – eine endlose Geschichte

Wiederholt berichtete die DSK über die Bestrebungen, die routinemäßige ärztliche Untersuchung von Asylbewerbern zu regeln. Zunächst beabsichtigte das Ministerium für Umwelt und Gesundheit, im Blick auf zwingende seuchenhygienische Gründe eine Verwaltungsvorschrift zu erlassen, die nähere Verfahrensbestimmungen enthalten sollte. Die DSK forderte indessen wegen des Eingriffscharakters derartiger Untersuchungsmaßnahmen die Schaffung einer bundesrechtlichen Grundlage und wurde mit dieser Forderung durch den Bundesbeauftragten für den Datenschutz und später auch durch das Ministerium für Umwelt und Gesundheit unterstützt. Die Bemühungen scheiterten, weil sich die Mehrheit der Länder für die Durchführung der Untersuchungen auf der Grundlage von Angebotsuntersuchungen – also gegen obligatorische Untersuchungen – aussprach (vgl. 12. Tb, Tz. 9.8.3). Das Ministerium äußerte in einer Sitzung des Ausschusses für Seuchenhygiene im September 1989 Zweifel, ob ärztliche Untersuchungen von Asylbewerbern – obligatorisch oder freiwillig – überhaupt zum Schutze der öffentlichen Gesundheit notwendig seien.

Gleichwohl legte es im August 1990 den neuen Entwurf einer Verwaltungsvorschrift für die gesundheitliche Betreuung von Asylbewerbern durch die Gesundheitsämter zur Beurteilung unter datenschutzrechtlichen Gesichtspunkten vor. Dieser Entwurf sah unter Aufgabe der früheren Forderung nach routinemäßigen (obligatorischen) Untersuchungen freiwillige Gesundheitsuntersuchungen für Asylbewerber vor. Im übrigen lehnte er sich inhaltlich weitgehend an eine entsprechende baden-württembergische Verwaltungsvorschrift an.

In einer Besprechung mit Vertretern der beteiligten Ressorts unterbreitete die DSK Vorschläge, die darauf zielten, daß Asylbewerber über Umfang und Bedeutung der Einwilligungserklärung aufgeklärt und Datenübermittlungen zwischen den Gesundheitsämtern und anderen Behörden auf das zur Aufgabenerfüllung erforderliche Minimum reduziert werden.

Auch diese Verfahrensregelung durch Verwaltungsvorschrift wird indessen, so wurde bekannt, nicht mehr weiterverfolgt. Der LfD erhielt Kenntnis von Bestrebungen, das Problem durch die Einführung von Vordrucken für die Datenerhebung und -übermittlung zu lösen. In einer Besprechung hat der LfD auf die Grundsatzforderungen verwiesen, die auch schon im Rahmen der datenschutzrechtlichen Beurteilung des Entwurfs einer Verwaltungsvorschrift erhoben wurden.

Nach Lage der Dinge besteht wenig Hoffnung, daß in absehbarer Zeit eine vertretbare Lösung gefunden wird. Weder ist zu erwarten, daß sich das Ministerium, seiner im Ausschuß für Seuchenhygiene geäußerten Auffassung folgend, darauf verstehen wird, die gegenwärtige Praxis zu ändern, noch wird die notwendige Rechtsgrundlage für diese Praxis geschaffen oder ein Verfahren eingeführt, das die Durchführung der Untersuchungen von der informierten Einwilligung der Betroffenen abhängig macht.

Die Einführung von Vordrucken mag einen Beitrag zur Rationalisierung von Verwaltungsarbeit leisten, das Kernproblem löst sie nicht.

13 Finanzverwaltung

13.1 Abgabenordnung (AO)

Die Abgabenordnung (AO) als verfahrensrechtliche Grundlage nicht nur der Steuererhebung durch die Landesfinanzbehörden, sondern auch durch Bundesbehörden und durch Gemeinden ist unter datenschutzrechtlichen Gesichtspunkten von erheblicher Bedeutung. Die Datenschutzbeauftragten haben seit langem ihre Ergänzung um bereichsspezifische datenschutzrechtliche Regelungen gefordert.

13.1.1 Struktur der datenschutzrechtlichen Ergänzung, Kompetenzen der Datenschutzbeauftragten

Das Verfahren zur datenschutzrechtlichen Ergänzung der Abgabenordnung ist nunmehr in ein neues Stadium eingetreten: Mit dem Erlaß der einschlägigen Vorschriften ist in absehbarer Zeit zu rechnen.

Die Entwicklung in diesem Zusammenhang ist für den Datenschutz positiv:

Der erste bekanntgewordene Referentenentwurf sah noch vor, daß die Datenschutzbeauftragten die Einhaltung des Steuergeheimnisses und generell Datenübermittlungen im Steuerbereich überhaupt nicht überprüfen dürften.

Dies hat das BDSG inzwischen ausdrücklich anders geregelt (§24 Abs. 2 Satz 1 BDSG).

In den folgenden Referentenentwürfen zur AO sind die Anliegen der Datenschutzbeauftragten zunehmend berücksichtigt worden. Der letzte grundsätzliche Konfliktpunkt ist inzwischen zufriedenstellend gelöst: Zunächst war geplant, die Kompetenzen der Landesbeauftragten für den Datenschutz im Finanzbereich identisch zu gestalten mit denen des Bundesbeauftragten für den Datenschutz gegenüber Bundesbehörden. Aufgrund des einhelligen Widerstandes der Landesbeauftragten für den Datenschutz ist das Bundesfinanzministerium nun auch an diesem Punkt kompromißbereit und wird einen Referentenentwurf vorlegen, der nur noch für die materiellen Datenverarbeitungsvorschriften das Bundesdatenschutzgesetz für ergänzend anwendbar erklärt:

- Wesentliche Datenverarbeitungs- und -nutzungsregelungen werden in der AO selbst bereichsspezifisch geregelt.

- Ergänzend ist für den Bereich der Datenverarbeitung und -nutzung das Bundesdatenschutzgesetz anzuwenden, soweit nicht die Gemeinden als Steuerbehörden tätig werden.

- Für die Befugnisse der Landesdatenschutzbeauftragten gegenüber den öffentlichen Stellen der Länder, soweit durch diese die Abgabenordnung anzuwenden ist, gelten die landesrechtlichen Bestimmungen, abgesehen von §§ 12 Abs. 3, 23 Abs. 4 und 24 Abs. 2 Satz 1 BDSG, die auch zugunsten der Landesbeauftragten für den Datenschutz Wirksamkeit entfalten sollen.

Zwischen Vertretern der Datenschutzbeauftragten und des Bundesministeriums der Finanzen hat ein umfassender Meinungsaustausch zu den Vorschriften im Detail stattgefunden, der eine weitgehende Annäherung der Standpunkte erbracht hat und jedenfalls zur Verbesserung des gegenseitigen Verständnisses wesentlich beigetragen haben dürfte. Der LfD hat das Finanzministerium Rheinland-Pfalz aufgefordert, bei den noch weiter erforderlichen Abstimmungen mit den Finanzverwaltungen des Bundes und der Länder dieses Ergebnis zu unterstützen.

Aus der Sicht des LfD sollte allerdings zur Erhöhung der Normenklarheit in § 31 b AOÄndG-Entwurf ausdrücklich bezeichnet werden, welche Bestimmungen des Bundesdatenschutzgesetzes ergänzend anzuwenden sind. Die für die Landesbeauftragten für den Datenschutz maßgeblichen Regelungen würden sich dann aus einer Ausnahmeregelung ergeben.

Dementsprechend könnte § 31 b AO etwa wie folgt lauten:

> (1) Soweit dieses Gesetz keine Regelungen trifft, sind für den Umgang mit personenbezogenen Daten in Verfahren, in denen dieses Gesetz von den Finanzbehörden anzuwenden ist, vorbehaltlich der Absätze 2 und 3 der 1. und 2. Abschnitt sowie §§ 39 und 43 des Bundesdatenschutzgesetzes anzuwenden. Dies gilt nicht für Verfahren, in denen dieses Gesetz von den Gemeinden anzuwenden ist oder soweit die Gemeinden Finanzbehörden sind.
>
> (2) Einzelangaben über persönliche oder sachliche Verhältnisse einer juristischen Person, einer nichtrechtsfähigen Personenvereinigung oder einer Vermögensmasse sowie Betriebs- und Geschäftsgeheimnisse, die dem Steuergeheimnis unterliegen, stehen den personenbezogenen Daten im Sinne des Bundesdatenschutzgesetzes gleich.
>
> (3) Die Vorschriften des 1. und 2. Abschnitts des Bundesdatenschutzgesetzes gelten abweichend von § 1 Abs. 2 Nr.1 des Bundesdatenschutzgesetzes auch, soweit der Datenschutz durch Landesgesetz geregelt ist. An die Stelle des Bundesbeauftragten für den Datenschutz treten insoweit die nach Landesrecht zuständigen Stellen; ihre Befugnisse gegenüber den in Absatz 1 genannten Stellen bestimmen sich ebenfalls nach Landesrecht. §§ 12 Abs. 3, 23 Abs. 4 und 24 Abs. 2 Satz 1 Bundesdatenschutzgesetz bleiben unberührt.

Die Diskussion hierzu ist noch nicht abgeschlossen.

13.1.2 Datenschutzrechtlich bedeutsame Einzelregelungen in der AO

a) Die DSK hatte sich intensiv darum bemüht, bei Beteiligungen an Publikumsgesellschaften zu ermöglichen, die gesonderten und einheitlichen Gewinnfeststellungsbescheide so auszugestalten, daß die steuerrechtlich relevanten Verhältnisse der Mitgesellschafter nicht jedem einzelnen Gesellschafter bekanntzumachen sind.

   Dieses Anliegen soll mit dem jetzt vorliegenden Gesetzentwurf aufgegriffen werden: Eine Einzelbekanntgabe soll in solchen Fällen grundsätzlich möglich sein. § 183 Abs. 1 AO soll entsprechend geändert werden. Der LfD begrüßt dies.

b) In § 116 AO wird angeordnet, daß grundsätzlich jede Behörde bei Verdacht einer Steuerstraftat das zuständige Finanzamt zu informieren hat. Eine Ausnahme gilt nur dann, wenn durch diese Information das Post- und Fernmeldegeheimnis des Artikel 10 GG beeinträchtigt werden könnte. Aus der Sicht des LfD müssen auch sonstige besondere Geheimhaltungsvorschriften (insbesondere das Arztgeheimnis) vor der Informationsweitergabe durch die verpflichtete übermittelnde Behörde zumindest berücksichtigt werden können Ansonsten wäre das Gesundheitsamt beispielsweise verpflichtet, bei Gesund-

heitsuntersuchungen von Arbeitnehmern jeden Verdacht der Schwarzarbeit dem Finanzamt zu melden. Auch bei der Gesundheitsuntersuchung von Prostituierten könnten Probleme im Zusammenhang mit dieser Meldepflicht auftreten. Das Bundesfinanzministerium hat eine Prüfung des datenschutzrechtlichen Anliegens des LfD zugesagt.

c) Auch Finanzamtsangehörige selbst haben ein Recht auf Datenschutz: Sie können dann in eine schwierige Situation geraten, wenn sie im Bezirk des Finanzamts wohnen, in dem sie beschäftigt sind. Dann hat nach der geltenden Rechtslage der Finanzamtsvorsteher persönlich, der auch Dienstvorgesetzter ist und über Beförderungen und sonstige Personalmaßnahmen zu entscheiden hat, die steuerlichen Unterlagen zur Kenntnis zu nehmen. Hier besteht die Gefahr, daß Informationen, die dem Steuergeheimnis unterliegen, zu Personalverwaltungszwecken verwendet werden. Der LfD hat angeregt, § 27 AO so zu ändern, daß auf Wunsch der Finanzamtsangehörigen ein anderes Finanzamt als das Beschäftigungsfinanzamt für die Besteuerung zuständig wird. Insofern sollte ein gesetzlicher Anspruch der betroffenen Finanzamtsbediensteten geschaffen werden. Auch diesbezüglich hat das Bundesfinanzministerium eine Überprüfung zugesagt.

d) In bezug auf die Übersendung von Steuermeßbescheiden an die Gemeinden (vgl. dazu 12. Tb, Tz. 14.5) hat sich leider keine Annäherung der Standpunkte ergeben. Mit Verwunderung hat der LfD allerdings zur Kenntnis genommen, daß maßgebliche Ausführungen des Rheinland-Pfälzischen Städtetages zu diesem Problem vom Finanzministerium zwar an das Bundesfinanzministerium weitergeleitet worden sind, daß die DSK jedoch über diese Stellungnahme nicht informiert worden ist und von diesen inhaltlichen Argumenten, die auch für die Meinungsbildung des LfD bedeutsam sind, erst durch den Bundesbeauftragten für den Datenschutz zwei Jahre später erfahren hat, obwohl sie die Diskussion zu diesem Punkt in Gang gebracht hat.

   Der LfD geht davon aus, daß es möglich wird, im Verhältnis zu allen Ressorts ein Klima zu schaffen, das eine solche Unterlassung künftig grundsätzlich ausschließt.

13.2 Kontrollmitteilungsverordnung

Sowohl im Interesse einer gerechten Besteuerung wie im Interesse der Normenklarheit ist es erforderlich, daß gemäß § 93 a AO eine Rechtsverordnung erlassen wird, die genau bestimmt, welche anderen öffentlichen Stellen unter welchen Voraussetzungen die Finanzämter über die Auszahlung von Leistungen an steuerpflichtige Personen und Stellen zu informieren haben (vgl. hierzu 12. Tb, Tz. 14.3, S. 74).

Nunmehr hat sich ergeben, daß die Verzögerung beim Erlaß dieser Verordnung darauf beruht, daß die Länder daran interessiert sind, daß entsprechende Kontrollmitteilungen auch Angaben über die Beträge der ausgezahlten Bezüge enthalten. Der Wortlaut des § 93 a AO läßt jedoch nur die Mitteilung der Tatsache von Auszahlungen als solcher zu. Die Länder haben vor Erlaß einer Kontrollmitteilungsverordnung auf einer Änderung der AO bestanden, damit die genannte Verordnung auch vorsehen kann, daß die Höhe der jeweiligen Auszahlungen an die Finanzämter mitgeteilt werden kann.

Aus der Sicht des LfD ist es datenschutzrechtlich nicht zwingend erforderlich, das Gesetz so auszugestalten, daß diese Information unterbleibt. An dieser Frage sollte jedenfalls der Erlaß der vorgesehenen Kontrollmitteilungsverordnung nicht scheitern.

13.3 Eingaben

Die Eingaben im Zusammenhang mit Datenschutzfragen im Bereich der Steuerverwaltung hatten schwerpunktmäßig folgende Fragen zum Inhalt:

- Rücksendung von Belegen durch das Finanzamt an Steuerpflichtige,
- Offenbarung von sensiblen Daten an den neuen Arbeitgeber durch die Vorlage der Steuerkarte,
- unzureichende Aktenzerkleinerungen im Finanzamtsbereich,
- Eintragung der Religionszugehörigkeit auf der Lohnsteuerkarte des Ehegatten.

13.3.1 Rücksendung von Belegen

Die Frage, in welchem Umfang das Finanzamt die Vorlage von Originalbelegen zum Nachweis steuerlich relevanter Tatbestände verlangen kann und wie sichergestellt werden kann, daß solche Originale nicht verloren gehen, war Gegenstand einer Eingabe. Der Beschwerdeführer trug vor, von ihm dem Finanzamt zugesandte Originalbelege seien ihm nicht zurückgeschickt worden. Eine Überprüfung des Verfahrensablaufs im Finanzamt hat ergeben, daß dort wie folgt vorgegangen wird:

- Bei der Prüfung der Steuererklärung werden die Angaben des Steuerbürgers anhand der eingereichten Belege auf Vollständigkeit und Schlüssigkeit nachvollzogen. Zusammen mit der abschließenden Zeichnung der Steuererklärung werden die Belege nach interner Aktenverfügung (die auf der Rückseite des Einkommensteuererklärungsvordruckes im Verfügungsteil

enthalten ist) an den Steuerbürger zurückgegeben. Der zuständige Sachbearbeiter ist mit Namenszeichen und Datum aus der Verfügung festzustellen. Die Belege werden im noch unverschlossenen Kuvert an die Poststelle weitergeleitet. Diese verschließt die Kuverts und leitet sie der Bundespost zu. Von der Poststelle werden keine Nachweise über ausgehende Postsendungen gefertigt.

- Die Oberfinanzdirektion Koblenz hat ausgeführt, das bisher praktizierte Verfahren habe sich bewährt. Beschwerden wegen verlorengegangener Postsendungen bei der Rücksendung von Belegen seien so gut wie unbekannt. Die Führung von Postausgangsbüchern sei zu arbeitsintensiv. Darüber hinaus seien solche Maßnahmen auch wegen der Vielzahl von ausgehenden Sendungen nicht praktikabel. Im übrigen verlange die Finanzverwaltung im Normalfall nicht die Vorlage von Originalbelegen. Im Regelfall reiche eine Kopie aus.

Diese Erwägungen sind auch aus datenschutzrechtlicher Sicht nicht unangemessen. Um jedes Risiko eines Verlustes auszuschließen, kann empfohlen werden, dem Finanzamt von besonders wichtigen Originaldokumenten grundsätzlich nur Kopien zur Verfügung zu stellen. In den Fällen, in denen das Finanzamt auf Originale nicht verzichten kann, könnten diese gelegentlich einer persönlichen Vorsprache beim Finanzamt vorgelegt werden.

13.3.2 Offenbarung sensibler Daten durch die Vorlage der Lohnsteuerkarte beim Wechsel des Arbeitgebers

Mehrere Anfragen haben den Bereich betroffen, daß beim Wechsel des Arbeitgebers der neue Arbeitgeber die alte Lohnsteuerkarte zur Kenntnis erhält. Dabei erfährt der neue Arbeitgeber, welche anderen Arbeitgeber der betroffene Arbeitnehmer im laufenden Steuerjahr gehabt hat sowie welche Bezüge er erhalten hat.

Das Anliegen der Bürger in diesem Zusammenhang ist aus datenschutzrechtlicher Sicht durchaus berechtigt: Die Übermittlung dieser Informationen an den neuen Arbeitgeber ist zu Besteuerungszwecken nicht unabdingbar nötig, dies folgt vielmehr aus der Eigenart der praktischen Durchführung des Lohnsteuerverfahrens. Dieses Verfahren erfordert, daß die Lohnsteuerkarte einen lückenlosen Überblick über die Zeiten der Beschäftigung und die erzielten Einkünfte ermöglicht. Praktikable Vorschläge, hier verfahrenstechnisch Abhilfe zu schaffen, sind bisher noch nicht entwickelt worden. Ein Bürger hat vorgeschlagen, den Arbeitgeber auf der Lohnsteuerkarte zu kodieren, oder den Namen abzudecken, um zu verhindern, daß der spätere Arbeitgeber Kenntnis vom vorherigen Arbeitsverhältnis erhält. Diese Lösung scheint jedoch nicht praktikabel zu sein. Eine Kodierung würde keinen wirksamen Schutz bieten: Es kann Arbeitgebern nicht verwehrt werden, die jeweils ihnen selbst zugewiesene Codenummer weiterzugeben oder zu veröffentlichen. Eine praktikable Verfahrensweise, die Namensfelder der Arbeitgeber nach Eintragung abzudecken und erst das Finanzamt diese Eintragung wieder zur Kenntnis nehmen zu lassen, läßt sich nur schwer vorstellen.

Derzeit haben die Betroffenen nur die Möglichkeit, weitere Lohnsteuerkarten mit der Steuerklasse VI einzusetzen. Damit sind jedoch finanzielle Nachteile verbunden, da eine Feststellung der tatsächlichen Steuerschuld erst nach Ablauf des Jahres im Rahmen der Einkommensteuerveranlagung oder des Lohnsteuerjahresausgleichs erfolgen kann.

Vor diesem Hintergrund bleibt es ein datenschutzrechtliches Anliegen, in diesem Bereich Verbesserungen zu erzielen. Die Finanzverwaltung sollte sich um eine Lösung dieser Fragen weiter bemühen und praktikable Alternativen entwickeln.

13.3.3 Eintragungen auf der Lohnsteuerkarte im Zusammenhang mit der Religionszugehörigkeit

Ein Bürger trug folgenden Sachverhalt vor:

Er sei aus der Kirche ausgetreten. Die Änderung seiner Lohnsteuerkarte sei ihm von der Lohnsteuerkartenstelle der Stadtverwaltung verweigert worden, da er die Lohnsteuerkarte seiner Ehefrau nicht gleichzeitig zur Änderung vorgelegt habe. Er sei aber vorerst nicht bereit, den Arbeitgeber seiner Frau über seinen Kirchenaustritt zu informieren. Insoweit sei er bereit, die bisherige Kirchensteuer weiter zu bezahlen.

Es ergab sich, daß aufgrund der bestehenden gesetzlichen Regelungen die Religionszugehörigkeit des Arbeitnehmers und seines Ehegatten jeweils auf der Lohnsteuerkarte einzutragen sind. Die Änderungseintragungen können nach den von der Oberfinanzdirektion Koblenz gegebenen Erläuterungen nicht auf die Lohnsteuerkarte eines Ehegatten beschränkt werden, da die Bemessung der Kirchensteuer je nach Zugehörigkeit zu einer steuerberechtigten Kirche unterschiedlich geregelt ist. Bei Ehegatten, die beide kirchensteuerpflichtig sind und die dem Steuerabzug vom Arbeitslohn unterliegen, bemißt sich die Kirchensteuer für den einzelnen Ehegatten nach der Hälfte der Lohnsteuer beider Ehegatten. Dagegen ist in den Fällen, in denen ein Ehegatte keiner steuerberechtigten Religionsgemeinschaft angehört, die Kirchensteuer lediglich nach der Lohnsteuer des kirchensteuerpflichtigen Ehegatten zu berechnen.

Es war dem LfD in diesem Zusammenhang nicht möglich, eine praktikable Alternative zu diesem – auf den Kirchensteuergesetzen beruhenden – Verfahren vorzuschlagen, das dem grundsätzlich verständlichen Anliegen des Bürgers gerecht geworden wäre.

13.3.4 Aktenvernichter bei den Finanzämtern

Aufgrund einer Eingabe wurde bekannt, daß bei den Finanzämtern Aktenvernichter im Einsatz sind, die den datenschutzrechtlichen Anforderungen nicht voll entsprechen. Der Beschwerdeführer hatte während eines Pokerabends die dort ausgestreuten Papierreste genauer angesehen und bemerkt, daß auch Überreste aus Steuerlisten auf diese Weise zweckentfremdet worden waren. Die Papierstreifen ließen noch Namen und Steuernummern von steuerpflichtigen Personen erkennen.

Die OFD hat auf Initiative der DSK veranlaßt, daß künftig entsprechende steuerliche Unterlagen so in die Aktenvernichter eingegeben werden, daß keine Zeilen mehr erkennbar sind.

Aus datenschutzrechtlicher Sicht ist allerdings gerade bei Unterlagen, die sensible Daten enthalten, der Einsatz effektiverer Aktenvernichter zu fordern, die mit der Technik des „cross-cutting" ausgestattet sind und die eingegebenen Papiere in unleserliche Reste zerkleinern. Aus Kostengründen hat die OFD hiervon zunächst abgesehen. Künftige Ersatzbeschaffungen werden dieser Anforderung jedoch gerecht werden müssen.

Im konkreten Fall war nicht mehr aufklärbar, auf welchem Wege die Papierreste vom Finanzamt zum Polterabend gelangt sind.

14 Wirtschaft und Verkehr

14.1 Datenverarbeitung im Zusammenhang mit dem Führen und Halten von Kraftfahrzeugen

14.1.1 Zentrales Verkehrsinformationssystem beim Kraftfahrtbundesamt in Flensburg (ZEVIS)

ZEVIS ist das zentrale Halterregister in der Bundesrepublik. Hier ist jeder Kfz-Halter mit bestimmten, gesetzlich festgelegten Daten in einem automatisierten System erfaßt. Die datenschutzrechtlichen Anforderungen und deren Umsetzung in den entsprechenden Gesetzen sind von der DSK in ihrem 12. Tätigkeitsbericht beschrieben worden (Tz. 11.1).

Im Berichtszeitraum war es Aufgabe der Datenschutzkontrollbehörden, auf eine exakte Einhaltung der gesetzlichen Anforderungen in diesem Bereich zu achten, entstehende Schwierigkeiten bei der Anwendung datenschutzrechtlicher Vorschriften zur Kenntnis zu nehmen und ggf. Initiativen zur Abhilfe zu entfalten.

In bezug auf Direktabfragen durch rheinland-pfälzische Stellen beim zentralen Register in Flensburg haben sich insofern Probleme ergeben, als das automatisierte System keine umfassende Protokollierung der erfolgenden Abrufe vornimmt und in einigen Fällen, in denen der Verdacht unberechtigter Abrufe bestand, nicht mehr nachvollzogen werden konnte, welche Person zu welchem Zweck jeweils einen Abruf veranlaßt hat (vgl. oben Tz. 5.8).

Diese Gestaltung der Protokollierung entspricht der gesetzlichen Regelung; es ist auch zweifelhaft, ob angesichts der grundsätzlich nicht sehr hohen Sensitivität der gespeicherten Daten eine umfassende Protokollierung aller Abrufe angemessen wäre, da in Anbetracht der Vielzahl der Abrufe und der verhältnismäßig geringen Zahl problematischer Fälle, in denen eine Nachprüfung erforderlich ist, der Aufwand im Verhältnis zum datenschutzrechtlichen Nutzen wohl unangemessen wäre.

Über die laufenden Abrufe und die Organisation des Abrufverfahrens in Rheinland-Pfalz wurden folgende Erkenntnisse gewonnen:

Zentrale Ansprechstelle für die Vollzugspolizei des Landes Rheinland-Pfalz bezüglich des ZEVIS-Verfahrens ist das Landeskriminalamt. Hier befinden sich 64 Anschlüsse für Zugriffe durch die Polizeidienststellen. Das Kraftfahrtbundesamt erstellt monatlich Statistiken sowie Verzeichnisse der durchgeführten Protokollierungen. Diese werden dem Landeskriminalamt zur Verfügung gestellt, das eine Prüfung auf Auffälligkeiten durchführt. Die Listen werden zudem den Bezirksregierungen zur Überprüfung übersandt. Zusätzlich überprüft das LKA stichprobenartig die protokollierten Abfragen. Ein Verdacht auf mißbräuchliche Nutzung der Abrufe hat sich bislang nicht ergeben.

Ein Handlungsbedarf aus der Sicht des Datenschutzes ist in diesem Bereich derzeit nicht ersichtlich.

14.1.2 Direktabrufverfahren bei örtlichen Halterregistern

Neben dem zentralen Verkehrsinformationssystem bestehen örtliche Halterregister bei den jeweiligen Zulassungsstellen, die in Rheinland-Pfalz weitgehend automatisiert geführt werden. In der Vergangenheit war es üblich, daß Polizeidienststellen auf diese örtlichen Register unmittelbar zugegriffen haben, um auch Veränderungen, die im zentralen Register noch nicht eingetragen waren, berücksichtigen zu können. Dies geschieht derzeit nur noch in seltenen Ausnahmefällen. Ein Direktanschluß an automatisierte örtliche Halterregister besteht bei keiner rheinland-pfälzischen Zulassungsstelle mehr, denn dies ist grundsätzlich nicht mehr erforderlich, da das zentrale Fahrzeugregister nunmehr relativ schnell auch Veränderungen speichert. Soweit sich aus der Sicht des Ministeriums des Innern und für Sport sowie der Polizei dennoch ein Bedarf für derartige Direktanschlüsse ergibt, ist aus datenschutzrechtlicher Sicht insbesondere die Einhaltung der gesetzlich vorgeschriebenen Protokollierungen erforderlich.

14.1.3 Halterauskünfte durch Kfz-Zulassungsstellen an Private

Derzeit gilt die Regelung, daß an Private grundsätzlich nur dann Auskünfte aus dem Halterregister erteilt werden dürfen, wenn der Anfragende einen Rechtsanspruch geltend macht, der im Zusammenhang mit der Teilnahme am Straßenverkehr steht (§ 39 StVG). Insofern hat sich die Rechtslage verändert: Gem. § 26 Abs. 5 StVZO war früher die Geltendmachung eines berechtigten Interesses an der Auskunft ausreichend; dieses konnte sich aus jedem Lebenszusammenhang ergeben.

Eine enge Auslegung der neuen gesetzlichen Regelung ist aus datenschutzrechtlicher Sicht nicht erforderlich. So hat die DSK beispielsweise die Auffassung vertreten, daß eine Erforderlichkeit der Auskunft zur Durchsetzung eines Rechtsanspruchs im Zusammenhang mit der Teilnahme am Straßenverkehr auch dann vorliegt, wenn ein Hauseigentümer zivilrechtlich gegen Falschparker vorgehen möchte, die unberechtigterweise auf seinem Grundstück parken. Der ruhende Verkehr ist Teil des Begriffs „Straßenverkehr".

Ein solches berechtigtes Interesse liegt allerdings dann nicht vor – wie die DSK ebenfalls in verschiedenen Zusammenhängen vertreten hat –, wenn die Halterauskunft nur dazu dienen soll, den Halter unmittelbar ohne Einschaltung der Polizei auf Verkehrsverstöße eines Fahrers aufmerksam zu machen. Hier fehlt es am Merkmal der Erforderlichkeit zur Geltendmachung von Rechtsansprüchen: Eine Strafanzeige oder eine Ordnungswidrigkeitenanzeige kann durch den verletzten oder gefährdeten Verkehrsteilnehmer unter Angabe des betroffenen Kennzeichens bei der Polizei erstattet werden. Hierzu ist die Kenntnis des Namens des Fahrzeughalters nicht erforderlich. Es begründet keinen Rechtsanspruch i. S. d. § 39 StVG, wenn der gefährdete Verkehrsteilnehmer seinen Kontrahenten im Straßenverkehr unmittelbar ermahnen will und zu diesem Zweck eine Halterauskunft beantragt.

Problematisch in diesem Zusammenhang ist auch, welcher Überzeugungsgrad bei der Kfz-Zulassungsstelle über die Richtigkeit des Vorbringens des Fragestellers vorliegen muß. So sind dem LfD Fälle bekannt geworden, in denen bei einer Anfrage Behauptungen aufgestellt worden sind, die nur schwer überprüfbar waren und die die Vermutung zugelassen haben, daß der Fragesteller unter Vorspiegelung falscher Tatsachen Halterdaten erfahren wollte. So hat ein Gläubiger beispielsweise behauptet, er sei von dem Fahrzeug seines Schuldners im Straßenverkehr gefährdet worden, um nach Auskunfterteilung eine Pfändung des betreffenden Fahrzeuges durch den Gerichtsvollzieher zu veranlassen. In einem anderen Fall hat ein Bürger behauptet, ein ihm unbekanntes ständig vor der Haustür seiner geschiedenen Ehefrau parkendes Fahrzeug habe ihn gefährdet, um herauszufinden, ob seine geschiedene Ehefrau möglicherweise eine neue Beziehung aufgebaut hat.

Hier können jedoch die Anforderungen an die Nachforschungspflichten der Zulassungsstelle nicht überzogen werden. Grundsätzlich sind Halterdaten nicht so schutzbedürftig – und aufgrund der Funktion des Kfz-Kennzeichens als Anknüpfungspunkt für Maßnahmen aus der Teilnahme am Straßenverkehr auch nicht schutzfähig –, daß jeder Mißbrauch ausgeschlossen werden kann.

14.1.4 Vernichtung von Vorgängen über vorangegangene Fahrverbote und Fahrerlaubnisentzüge in der Führerscheinakte

Wiederholt wurden Anfragen an die DSK gerichtet, wann Vorgänge über fehlgeschlagene Versuche, die Fahrerlaubnis zu erhalten sowie über Fahrerlaubnisentzüge und Fahrverbote aus der Führerscheinakte zu entfernen sind.

In diesem Zusammenhang ist die DSK von folgender Rechtslage ausgegangen:

Führerscheinakten ohne belastende Vorgänge werden fünf Jahre seit der Erteilung der Fahrerlaubnis aufbewahrt.

Führerscheinakten mit Vorgängen, die mit der Entziehung einer Fahrerlaubnis in Zusammenhang stehen, werden zehn Jahre aufbewahrt. Dies gilt auch für Eignungsgutachten der medizinisch-psychologischen Untersuchungsstellen.

Informationen über die Entziehung einer Fahrerlaubnis wegen Trunkenheit werden außerdem im Verkehrszentralregister gespeichert. Entsprechende Angaben werden dort ebenfalls grundsätzlich zehn Jahre vorrätig gehalten. Eine Ausnahme gilt für Entscheidungen, mit denen die Erteilung einer Fahrerlaubnis für immer untersagt worden ist. Solche Informationen werden für unbestimmte Zeit gespeichert (§ 13 a Abs. 1 Satz 1 2. Halbsatz StVZO).

Vor Erteilung einer Fahrerlaubnis hat jede Erlaubnisbehörde beim Kraftfahrtbundesamt anzufragen, ob Nachteiliges über den Antragsteller bekannt ist.

Aufgrund einer Eingabe hat der LfD erfahren, daß diese Vorgaben nicht immer genau eingehalten werden. In einem Fall wurden Vorgänge, die zwanzig und siebzehn Jahre zurückgelegen haben, noch zum Gegenstand einer aktuellen Entscheidung der Fahrerlaubnisbehörde gemacht. Der LfD ist in Übereinstimmung mit einem Urteil des Bundesverwaltungsgerichts (vom 17. Dezember 1976, Az.: VII C 28.74) der Auffassung, daß bezüglich solcher Daten, die aufgrund der vorgenannten Fristen aus den Führerscheinakten zu entfernen sind, auch ein Verwertungsverbot für künftige Entscheidungen besteht.

14.2 Kartei der Gewerbeanmeldungen

In vorangegangenen Tätigkeitsberichten wurde wiederholt auf die Problematik hingewiesen, die für die automatisiert geführten Gewerberegister aus § 7 Abs. 1 LDatG folgt: Danach sind Auskünfte aus automatisierten Dateien an private Empfänger nur dann möglich, wenn entweder eine gesetzliche Vorschrift entsprechende Auskünfte ermöglicht oder wenn die betroffenen Bürger formgerecht zugestimmt haben.

Für automatisiert geführte Gewerbedateien existiert keine besondere Rechtsgrundlage, die Einholung der Einwilligung der betroffenen Gewerbetreibenden ist grundsätzlich vor einer Auskunftserteilung an Private nur schwer möglich und in vielen Fällen auch nicht sachdienlich (wenn etwa ein Gläubiger Informationen über einen Schuldner benötigt).

Zur praktischen Lösung der hier bestehenden Schwierigkeiten war die DSK damit einverstanden, daß die Ordnungsbehörden, die die Gewerbekarteien führen, in allgemeiner Form die betroffenen Gewerbetreibenden auf die Möglichkeit hinweisen, gegen die Auskunftserteilung an Private generell Widerspruch einzulegen. Bezüglich aller Gewerbetreibenden, die keinen Widerspruch eingelegt haben, könnte dann davon ausgegangen werden, daß diese mit Auskunftserteilungen einverstanden sind.

Bei einer datenschutzrechtlich zu engen Auslegung des Gesetzes wäre eine solche Verfahrensweise nicht zulässig; bei einer Abwägung der betroffenen Rechtsgüter ist jedoch auch der LfD der Ansicht, daß diese Vorgehensweise rechtmäßig ist. Dennoch bleibt nach wie vor eine entsprechende Ergänzung der Gewerbeordnung im Interesse der Rechtsklarheit wünschenswert. Zu Übermittlungen aus dem Gewerberegister an öffentliche Stellen s. unten Tz. 20.6.4 .

14.3 Datenübermittlungen durch Sparkassen an die Schufa

Der LfD ist auch für die datenschutzrechtliche Überwachung öffentlich-rechtlicher Wettbewerbsunternehmungen, zu denen insbesondere die Sparkassen zählen, zuständig. Eingaben in diesem Bereich bezogen sich insbesondere auf Datenübermittlungen an die Schufa.

In einem Fall hat die DSK entsprechende Übermittlungen für unverhältnismäßig gehalten. Der Beschwerdeführer war zwar mit Kreditrückzahlungen im Verzug und deshalb waren seine Kredite gekündigt worden, ein sog. „hartes Negativmerkmal" i. S. d. Schufa-Vertragsbedingungen (wie z. B. ein beantragter Mahnbescheid) lag jedoch nicht vor. Außerdem war es angesichts der zur Zeit der Datenübermittlung an die Schufa laufenden Umschuldungsverhandlungen zwischen dem Beschwerdeführer und der Sparkasse sowie Dritten für die DSK nicht nachvollziehbar, daß es zur Wahrung berechtigter Interessen der Sparkasse, eines Vertragspartners der Schufa oder der Allgemeinheit erforderlich gewesen wäre, entsprechende Informationen an die Schufa zu übermitteln.

Zu dieser Frage hat es einen intensiven Schriftwechsel mit der betroffenen Sparkasse gegeben. Der LfD ist der Auffassung, daß grundsätzlich auch bei der Beurteilung dieser Frage ein weiter Beurteilungsspielraum für die Sparkassen besteht; Datenschutzkontrolle muß hier zurückhaltend ausgeübt werden. Im konkreten Fall bestand jedoch ein enger zeitlicher Zusammenhang zwischen der Meldung an die Schufa sowie Umschuldungsverhandlungen, in deren Verlauf die Sparkasse durch eine Grundschuld abgesichert worden ist, so daß auch aus der Sicht des LfD eine deutliche Überschreitung dieses Beurteilungsspielraums vorlag. Angesichts der existenziellen Folgen einer Meldung von Negativmerkmalen an die Schufa muß dieser eine sorgfältige Abwägung der zu berücksichtigenden Interessen vorausgehen.

Die betroffene Sparkasse hat sich im Ergebnis dieser Auffassung angeschlossen und die Schufa gebeten, die fraglichen Meldungen von Anfang an zu löschen.

Aus der Sicht des LfD ist dies ein erfreuliches Zeichen dafür, daß die Sparkassen bereit sind, datenschutzrechtliche Anliegen ihrer Kunden sehr ernst zu nehmen.

15 Baurecht, Liegenschaftskataster

15.1 Städtebauliche Sanierungsmaßnahmen; Auskunftspflicht

§ 138 Abs. 1 Baugesetzbuch (BauGB) verpflichtet Eigentümer, Mieter, Pächter und sonstige zum Besitz oder zur Nutzung eines Grundstücks, Gebäudes oder Gebäudeteils Berechtigte sowie ihre Beauftragten, der Gemeinde oder ihren Beauftragten Auskunft über die Tatsachen zu erteilen, deren Kenntnis zur Beurteilung der Sanierungsbedürftigkeit eines Gebiets oder zur Vorbereitung oder Durchführung der Sanierung erforderlich ist. An personenbezogenen Daten können insbesondere Angaben der Betroffenen über ihre persönlichen Lebensumstände im wirtschaftlichen und sozialen Bereich, namentlich über die Berufs-, Erwerbs- und Familienverhältnisse, das Lebensalter, die Wohnbedürfnisse, die sozialen Verpflichtungen sowie über die örtlichen Bindungen, erhoben werden.

Das grundsätzliche Verwertungsverbot der Daten für andere als Sanierungszwecke nach Abs. 2 ist zugunsten der Finanzbehörden durchbrochen; verweigert ein Auskunftspflichtiger die Auskunft, kann nach Abs. 4 in entsprechender Anwendung von § 208 Satz 2 bis 4 BauGB ein Zwangsgeld angedroht und festgesetzt werden.

Der LfD vertritt die Auffassung, daß eine gesetzlich begründete, im Wege des Verwaltungszwangs durchsetzbare Auskunftspflicht ein höheres Maß an Normenklarheit erfordert. Die Erhebungsmerkmale sollten – auf das zur Erreichung des Zwecks notwendige Minimum beschränkt – im Gesetz möglichst exakt bezeichnet werden. Die Erhebung unzumutbarer Intimangaben muß ausgeschlossen werden. Eine Zweckentfremdung der Daten darf nur in Ausnahmefällen und nur dann in Betracht kommen, wenn der Betroffene hierauf ausdrücklich hingewiesen wurde. Die Bedingungen, unter denen die Daten verarbeitet und genutzt werden dürfen, sollten denen der amtlichen Statistik zumindest angenähert sein.

Diese Auffassung wurde dem Bundesbeauftragten für den Datenschutz mitgeteilt. Zugleich wurde angeregt, für normenklare Regelungen zur Auskunftspflicht im Baugesetzbuch einzutreten.

15.2 Vorkaufsrecht der Gemeinden

Zum Zwecke der Entscheidung über die Ausübung des gemeindlichen Vorkaufsrechts sind Grundstücksverkäufer oder -käufer nach § 28 Abs. 1 Satz 1 BauGB verpflichtet, der Gemeinde den Inhalt des Kaufvertrags unverzüglich mitzuteilen. In der Praxis werden diese Mitteilungspflichten zumeist durch die Notare wahrgenommen, die eine vollständige Ausfertigung des Kaufvertrags an die jeweilige Gemeinde übermitteln.

Der DSK wurde bekannt, daß es Gemeinden gibt, die auf die Übersendung der vollständigen Kaufverträge verzichten und sich mit Angaben begnügen, die zur Feststellung eines bestehenden Vorkaufsrechts erforderlich sind. Andere Gemeinden bestehen auf Übersendung der vollständigen Kaufverträge, obwohl die Ausübung eines gesetzlichen Vorkaufsrechts nur in weniger als 10 Prozent der Fälle in Betracht kommt und, nach den Ergebnissen einer Umfrage der Bundesnotarkammer, bundesweit nur in 0,07 Prozent aller angezeigten Kaufverträge das Vorkaufsrecht tatsächlich ausgeübt wird.

Die Übermittlung der in den Kaufverträgen enthaltenen personenbezogenen Daten und die Speicherung dieser Daten bei den Gemeinden in der Form einer Sammlung von Kaufverträgen begegnet angesichts der Tatsache, daß nur ein außerordentlich geringer Teil dieser Daten für die Aufgabenerfüllung tatsächlich erforderlich ist, datenschutzrechtlichen Bedenken. Bedenklich ist insbesondere die Nutzung dieser Daten für Abgabenzwecke (Berichtigung von Adreßdateien) oder für die Errichtung einer inoffiziellen Kaufpreissammlung.

Der DSK wurde bekannt, daß es der kommunalen Praxis z. B. in Bayern und Berlin entspricht, die Datenübermittlung zunächst auf wenige Grunddaten zu beschränken und den übrigen Inhalt des Kaufvertrags nur auf ausdrückliches Verlangen mitzuteilen.

Sie empfahl dem Ministerium des Innern, dieses sog. zweistufige Verfahren auch in Rheinland-Pfalz allgemein einzuführen.

Das Ministerium hat diesen Vorschlag aufgegriffen. Es bat die Kommunalen Spitzenverbände, das Verfahren ihren Mitgliedern zur Anwendung zu empfehlen.

Ergänzend wurde der Bundesbeauftragte für den Datenschutz eingeschaltet mit dem Anliegen, auf eine Änderung des § 28 Abs. 1 BauGB dergestalt hinzuwirken, daß das gestufte Übermittlungsverfahren auch gesetzlich vorgeschrieben wird.

15.3 Änderung des Landesgesetzes über das Liegenschaftskataster

Die Weiterentwicklung des Liegenschaftskatasters mit dem Ziel der Schaffung eines fachübergreifenden Informationssystems ist seit längerer Zeit in der Diskussion (vgl. 12. Tätigkeitsbericht, Tz. 17.2). Die DSK forderte klare Aufgabenbeschreibungen sowie gesetzliche Regelungen für die Datenerhebung und -verarbeitung; sie begrüßte es, daß das Ministerium des Innern die datenschutzgemäße Weiterentwicklung des Katastergesetzes im Rahmen eines Landesgesetzes zur Fortführung der Verwaltungsvereinfachung in Angriff nahm. Kernstück einer Novellierung des Katastergesetzes war eine gesetzliche Definition des Zwecks sowie die Neuregelung der Nutzungsbestimmungen. Darüber hinaus zielte ein der DSK zur Stellungnahme vorgelegter Entwurf auf eine Klarstellung des zulässigen Umfangs der Datenerhebung sowie des Inhalts des Liegenschaftskatasters.

Für kritikwürdig hielt die DSK die Verordnungsermächtigungen zur Regelung der Datenübermittlung. Dies insbesondere deshalb, weil der Zweck des Liegenschaftskatasters nur in einer sehr allgemeinen Form beschrieben war und die Ermächtigung, auch den Inhalt des Liegenschaftskatasters durch Rechtsverordnung festzulegen und fortzuschreiben, in dem zur Stellungnahme vorgelegten Entwurf noch keine näheren inhaltlichen Vorgaben enthielt. Die DSK wies auf die Wechselbeziehung der Vorschriften hin, die insoweit besteht, als eine genaue gesetzliche Bestimmung der in einem Register gespeicherten Daten – wie beispielsweise im Meldegesetz – durchaus eine Fassung der Verordnungsermächtigung zur Regelung von Datenübermittlungen zuläßt, die dem Verordnungsgeber einen großen Regelungsspielraum einräumt. Je geringer die Detailgenauigkeit bei der Bestimmung des Zwecks und des Inhalts ist, um so größere Anforderungen sind an die Bestimmtheit anderer Eingriffsregelungen zu stellen.

Die Überarbeitung des Entwurfs unter Berücksichtigung der Empfehlungen der DSK führte zu deutlichen Verbesserungen, die schließlich auch Eingang in das Gesetz fanden. Gleichwohl sind noch weitere Schritte in Richtung einer Konkretisierung von Zweck und Inhalt geboten. Entscheidend wird sein, in welcher Weise den Datenschutzforderungen bei der inhaltlichen Gestaltung der Rechtsverordnungen entsprochen wird. Das Ministerium hat zugesagt, die zu erlassenden Rechtsverordnungen rechtzeitig mit der DSK abzustimmen. Es ist davon auszugehen, daß diese Zusage auch gegenüber dem LfD gilt.

16 Statistik

16.1 Überführung der Kriminalstatistik der ehemaligen DDR in das Statistische Bundesamt

Der Bundesminister für Justiz hat im Einvernehmen mit dem Bundesminister des Innern vorgeschlagen, die Daten der Kriminalstatistik der ehemaligen DDR in das Statistische Bundesamt zu überführen. Gegen dieses Vorhaben sind nicht nur von Datenschutzkontrollbehörden, sondern auch von Fachbehörden für den Statistik- und Justizbereich Bedenken geäußert worden.

Diese Bedenken richten sich in erster Linie dagegen, daß es sich bei dieser sog. „Kriminalstatistik" tatsächlich um einen lückenlosen personenbezogenen Nachweis von Straftaten handelt, die nach dem Recht der ehemaligen DDR begangen wurden. Dieser Nachweis war dort Teil des zentralen Einwohnerregisters. Es ist anzunehmen, daß sich unter den gespeicherten Daten auch Angaben über solche strafbaren Handlungen befinden, die unter rechtsstaatlichen Bedingungen nicht zu einer Strafverfolgung oder Verurteilung geführt hätten. Da ohne Hinzuziehung von Akten eine Bewertung der gespeicherten Fälle nicht möglich sein dürfte, eine derartige aktenmäßige Überprüfung jedoch offensichtlich unmöglich ist, begegnet schon die weitere Speicherung der Daten erheblichen Bedenken.

Die nichtanonymisierte Überführung dieser Daten in das Statistische Bundesamt würde das informationelle Selbstbestimmungsrecht der Betroffenen zusätzlich unvertretbar beeinträchtigen.

Das Ministerium des Innern, das vom LfD um Stellungnahme gebeten wurde, teilte die Bedenken gegen die Übernahme der gespeicherten Daten durch das Statistische Bundesamt. Es wies darauf hin, daß die Daten der Kriminalstatistik der ehemaligen DDR für die Verbrechensbekämpfung in der Bundesrepublik ohne Bedeutung sind. Dies resultiere zum einen aus den unterschiedlichen strafrechtlichen Bestimmungen und zum anderen aus der lückenhaften statistischen Erfassung strafrechtlicher Vorgänge in der ehemaligen DDR, wo Straftaten nach dem Opportunitätsprinzip verfolgt und auch entsprechend statistisch behandelt wurden. Die Kriminalstatistik der ehemaligen DDR sei auch nicht annähernd ein Indikator für das Kriminalitätsaufkommen gewesen. Eine Nutzung der Daten für Forschungszwecke setze ein schlüssiges datenschutzrechtliches Konzept voraus.

16.2 Statistikgeheimnis

Durch eine Eingabe erhielt die DSK Kenntnis von folgendem Sachverhalt:

In einem Normenkontrollverfahren – Gegenstand war der Bebauungsplan einer Gemeinde – war die Frage von Bedeutung, welchen Viehbestand der Antragsteller in der Vergangenheit hatte. Der die Antragsgegnerin, eine Ortsgemeinde, in dem Ver-

fahren vertretende Rechtsanwalt trug in seinem Schriftsatz folgendes vor: „Bestritten wird, daß in der Vergangenheit jemals 250 Mastschweine gehalten worden sind. Dem Antragsteller mag aufgegeben werden, die jährlich zu statistischen Zwecken abgegebene Erklärung über den Viehbestand vorzulegen." Der Betroffene rügte dies als einen Verstoß gegen die Vorschriften zum Schutze des Statistikgeheimnisses.

Die DSK vertrat die Auffassung, daß der Erklärungsinhalt des Vorbringens dahingehend verstanden werden kann, daß sich die Unrichtigkeit von Angaben des Klägers im Verfahren aus seinen Angaben bei der amtlichen Statistik (Viehzählung) ergibt. Der Beweisantrag vermittelt den Eindruck, daß der Ortsgemeinde Erkenntnisse vorliegen, wonach der Antragsteller in zu statistischen Zwecken abgegebenen Erklärungen eine geringere Anzahl von Tieren – als im Normenkontrollverfahren behauptet – angegeben hat.

Die DSK wertete dies – in Übereinstimmung mit dem Statistischen Landesamt – als einen Verstoß gegen die Bestimmungen zum Schutze des Statistikgeheimnisses (§ 16 Bundesstatistikgesetz).

16.3 Landwirtschaftszählung 1991

Die Sensibilisierung der Bevölkerung für Datenschutzprobleme ist bei der Durchführung amtlicher Statistiken besonders groß. Die Nachwirkungen der öffentlichen Diskussion von Datenschutzfragen im Zusammenhang mit der Volkszählung 1987 sind deutlich erkennbar.

Bei der Landwirtschaftszählung 1991 (zugleich Agrarberichterstattung 1991) wurde in mehreren Eingaben an die Behörde des LfD bemängelt, daß Erhebungsvordrucke für diese Zählung durch gemeindliche Bedienstete offen zugestellt wurden. Eine vergleichbare Problematik stand auch im Mittelpunkt von Eingaben zur Volkszählung.

Es war jeweils darauf hinzuweisen, daß diese Verfahrensweise zulässig ist: Nach § 2 Abs. 1 Nr. 4 der Landesverordnung zur Durchführung des Agrarstatistikgesetzes vom 25. August 1989 hat die Erhebungsstelle die Erhebungsvordrucke „auszuteilen und einzusammeln". Eine gleichlautende Vorschrift enthält § 5 Abs. 1 Nr. 4 des Landesstatistikgesetzes. Die offene Zustellung ist unproblematisch, weil der Erhebungsbogen bei der Austeilung zwar Adreßangaben und einige für die organisatorische Durchführung bedeutsame Ordnungsziffern, aber noch keine Einzelangaben des Auskunftspflichtigen enthält. Für die Rückgabe der ausgefüllten Vordrucke sind nach § 15 Abs. 5 Bundesstatistikgesetz Verfahren zugelassen, die gewährleisten, daß Gemeindebedienstete als Erhebungsbeauftragte den Inhalt ausgefüllter Erhebungsvordrucke nicht zur Kenntnis nehmen können. Das Gesetz läßt die Übergabe im verschlossenen Umschlag an den Erhebungsbeauftragten sowie die unmittelbare Übergabe oder Übersendung an die Erhebungsstelle zu, trägt also bestehenden Geheimhaltungsinteressen Rechnung.

16.4 Statistik der Jugendhilfe

Da in fast allen Bereichen der öffentlichen Verwaltung personenbezogene Daten erhoben und genutzt werden, sind die Kontroll- und Beratungsaufgaben des LfD entsprechend weit gespannt. Gleichwohl ist es geboten, bei der Datenschutzarbeit zu beachten, daß sie ihren Bezugspunkt in den Persönlichkeitsrechten der Bürger hat. Sind diese beeinträchtigt, ist es die Aufgabe der Datenschutzkontrolle, mit allen zur Verfügung stehenden Mitteln auf die Herstellung eines gesetzeskonformen Zustandes hinzuwirken. Werden Persönlichkeitsrechte nicht berührt, steht es der Datenschutzkontrolle nicht zu, die Rechtmäßigkeit von Datenverarbeitungsvorgängen zu beurteilen.

An dem folgenden Beispiel wird dargestellt, welche Zielkonflikte in der Praxis entstehen können.

Das Land Rheinland-Pfalz fördert soziale Beratungsstellen freier und öffentlicher Träger mit den Beratungsangeboten Erziehungsberatung, Ehe-, Familien- und Lebensberatung, Suchtberatung sowie soziale Beratung Schwangerer durch die Zahlung von Zuschüssen. Zuständige Stelle ist das Landesamt für Jugend und Soziales. Diese Behörde möchte natürlich auch wissen, welche Leistungen erbracht wurden; hierzu werden Informationen bei den Beratungsstellen erhoben. Es liegt nahe, diesen Informationsbedarf so weit wie möglich dadurch abzudecken, daß der mittelbewilligenden Stelle Daten aus der amtlichen Kinder- und Jugendhilfestatistik nach §§ 98 ff. Kinder- und Jugendhilfegesetz (KJHG) zur Verfügung gestellt werden. Der LfD wurde gebeten, zu der Frage Stellung zu nehmen, ob dies zulässig sei.

Eine datenschutzrechtliche Überprüfung führte zu dem Ergebnis, daß die von den Beratungsstellen an das Statistische Landesamt übermittelten Einzeldatensätze eine Identifizierung von Klienten nicht zulassen. Auch für das Landesamt für Jugend und Soziales wären Betroffene – würden die Daten übermittelt – nicht identifizierbar. Gesichtspunkte des Datenschutzes stehen also einer Nutzung von Statistikdaten als Verwendungsnachweis für die Mittelbewilligung nicht entgegen.

Die Übermittlung von Statistikdaten an das Landesamt als „obere Landesbehörde" sowie die Zweckbestimmung dieser Datenübermittlung könnten indessen aus anderen als Datenschutzgründen bedenklich sein. § 103 KJHG bestimmt nämlich, daß

Daten nur an die fachlich zuständigen „obersten" Landesbehörden und nur für die Verwendung gegenüber den gesetzgebenden Körperschaften und für Zwecke der Planung, jedoch nicht für die Regelung von Einzelfällen übermittelt werden dürfen.

Im Blick auf die grundsätzliche Zuständigkeitsbegrenzung hat sich der LfD darauf beschränkt, auf den aus dieser Vorschrift möglicherweise zu entnehmenden Hinderungsgrund für die Verwendung der Statistikdaten hinzuweisen; er sah aber keine Veranlassung, das Vorhaben umfassend und abschließend zu würdigen.

17 Personaldatenverarbeitung

17.1 Einleitung

Im Bereich der Personaldatenverarbeitung ist der LfD häufig von Personalräten mit der Bitte angesprochen worden, Dienstvereinbarungen über automatisierte Personaldatenverarbeitungssysteme, insbesondere Zeiterfassungssysteme und Telefondatenerfassungssysteme, datenschutzrechtlich zu beurteilen.

- Auch der Bereich der Video-Überwachung von Diensträumen und Garagen hat in diesem Zusammenhang eine Rolle gespielt.

Zu diesen Fragen hat ein Meinungsaustausch mit der Technologie-Beratungsstelle des DGB in Mainz stattgefunden, deren Aufgabe die Beratung von Betriebs- und Personalräten im Zusammenhang mit der Einführung der automatisierten Datenverarbeitung ist. Es wurde vereinbart, insoweit künftig Möglichkeiten der Zusammenarbeit zu suchen und zu nutzen.

Aus datenschutzrechtlicher Sicht ist es vorrangig, die Grundsätze des Personalaktenrechts und der automatisierten Personaldatenverarbeitung gesetzlich bereichsspezifisch für den öffentlichen Dienst zu regeln (zu den Besonderheiten des öffentlichen Dienstes s. u. Tz. 17.3). Die derzeitige Rechtslage ist inhaltlich und formal nicht befriedigend:

Am 1. Juni 1991 ist das BDSG in der Fassung in Kraft getreten, die es durch das Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990 (BGBl. 90, 2954) erhalten hat. § 2 Abs. 3 LDatG verweist für dienst- oder arbeitsrechtliche Rechtsverhältnisse der Bediensteten öffentlicher Stellen des Landes auf die §§ 23 und 24 Abs. 1 sowie §§ 25 – 27 BDSG „in der jeweils geltenden Fassung".

Es ist zweifelhaft geworden, in welchem Umfang diese Verweisungen sinngemäß das neue BDSG betreffen und welche materiellen Änderungen dadurch für die betroffenen Stellen eingetreten sind.

In Übereinstimmung mit dem Ministerium des Innern und für Sport vertritt der LfD die Auffassung, daß anstelle der §§ 5, 6, 7, 12 und 13 des LDatG im Bereich der dienst- oder arbeitsrechtlichen Rechtsverhältnisse die §§ 28 Abs. 1 und 2 Nr. 1 Satz 1 sowie die §§ 33 – 35 BDSG gelten. Es ist zwar aus datenschutzrechtlicher Sicht erforderlich, eine entsprechende Klarstellung ausdrücklich in das LDatG aufzunehmen. Dennoch sollte im Interesse einer einheitlichen Rechtsanwendung schon vor einer solchen Gesetzesänderung davon allgemein ausgegangen werden, daß die §§ 28 Abs. 1 und 2 Nr. 1 Satz 1 sowie die §§ 33 bis 35 BDSG anzuwenden sind.

Für die Bediensteten im öffentlichen Bereich ergeben sich insbesondere Verbesserungen ihres Auskunftsanspruchs (§ 34 BDSG).

Die Ressorts sind darum gebeten worden, die ihnen nachgeordneten Behörden und Stellen über diese Rechtslage zu informieren.

17.2 Stand der gesetzgeberischen Initiativen

17.2.1 Vorliegende Regelungen und Gesetzentwürfe

Der Europarat hat am 18. Januar 1989 eine Empfehlung zum Schutz personenbezogener Daten für Beschäftigungszwecke (Nr. R [89] 2) verabschiedet. Diese Empfehlung ist für die Mitgliedsstaaten nicht verbindlich; sie knüpft außerdem nur an die automatisierte Verarbeitung personenbezogener Daten an. Vorgaben für die Personaldatenverarbeitung in Akten sind ihr also grundsätzlich nicht zu entnehmen.

Dennoch enthält diese Empfehlung wichtige Gesichtspunkte, die insbesondere für die nationalen Gesetzgeber Bedeutung haben. Allein die Existenz einer solchen Empfehlung beweist, daß Datenschutz bei Beschäftigungsverhältnissen auch im europäischen Rahmen besondere Beachtung gefunden hat und daß ein Tätigwerden der deutschen Gesetzgebung in diesem Bereich dringlich ist.

Der LfD begrüßt ausdrücklich das Vorhaben, in einem Gesetz zur Änderung dienstrechtlicher Vorschriften datenschutzrechtliche Vorgaben für den Bereich der Personalakten festzulegen (Entwurf eines 9. Gesetzes zur Änderung dienstrechtlicher Vorschriften, Gesetzentwurf der Bundesregierung vom 30. März 1990, Bundesratsdrucksache 223/90). Es wird erwartet, daß dieses Gesetz unter Berücksichtigung der von seiten der Datenschutzbeauftragten formulierten Änderungswünsche (vgl. hierzu insbesondere den 12. Tb, Anlage 6 sowie Anlage 1 zu diesem Tb) in naher Zukunft verabschiedet wird.

17.2.2 Regelungen zur Genomanalyse bei Arbeitnehmern

Auf der XIII. Internationalen Konferenz der Datenschutzbeauftragten, die zu Anfang Oktober 1991 in Straßburg stattfand, wurden die besonderen Gefahren angesprochen, die mit einer Verwendung der Genomanalyse im Arbeitsverhältnis zwangsläufig verbunden sind. Der Arbeitskreis Gentechnologie der Datenschutzbeauftragten des Bundes und der Länder hatte sich dieses Problembereichs schon zuvor angenommen. Die Gefährdungen im einzelnen sind – soweit heute schon überschaubar – u. a. im Bericht der Bundesregierung über die Umsetzung des Beschlusses des Deutschen Bundestages zum Bericht der Enquete-Kommission „Chancen und Risiken der Gentechnologie" (siehe Bundestagsdrucksache 11/8520 vom 5. 12. 1990 – Kap.9 S. 19 ff.) dargestellt. Jetzt liegt auch dem US-amerikanischen Kongreß der Entwurf eines Gesetzes zum Schutz des menschlichen Genoms bei Bundesbehörden vor. Die Zeit für eine gesetzliche Regelung drängt, denn mit der Bereitstellung geeigneter Untersuchungsverfahren ist bereits in wenigen Jahren zu rechnen.

Jede Regelung für den Arbeitsbereich wird die besondere abhängige Situation von Arbeitnehmern, aber auch von Bewerbern um einen Arbeitsplatz zu berücksichtigen haben. Von Freiwilligkeit bei der Einwilligung zur Durchführung von Tests und ihrer Auswertung in diesem Bereich kann grundsätzlich nicht gesprochen werden. Zur Sicherung eines Verbots muß auch die Einführung strafrechtlicher Sanktionen erwogen werden.

Die DSK hat seit ihrem Bestehen dem Schutz medizinischer personenbezogener Daten erhebliche Bedeutung beigemessen; der LfD stimmt mit dieser Gewichtung überein. Die Behandlung des Themas ‚Genomanalyse im Arbeitsverhältnis' wird also einen der Schwerpunkte der Arbeit des Datenschutzes auch auf der Landesebene darstellen. Schon jetzt sollte unbeschadet späterer gesetzlicher Regelungen Übereinstimmung darüber erzielt werden, daß durch öffentliche Stellen des Landes als Arbeitgeber oder Dienstherr die Genomanalyse grundsätzlich nicht genutzt werden darf.

17.3 Grenzen des Rechts auf informationelle Selbstbestimmung für Amtsträger

17.3.1 Reichweite des grundrechtlichen Schutzes der informationellen Selbstbestimmung

Die Frage, ob und in welchem Umfang sich Amtsträger auf „Datenschutz" oder das Recht auf informationelle Selbstbestimmung berufen können, ist grundsätzlicher Natur und weitgehend noch ungeklärt bzw. kontrovers. Sie ist in den verschiedensten Zusammenhängen bedeutsam, insbesondere auch für die Frage, welchen Gestaltungsspielraum der Gesetzgeber für bereichsspezfische gesetzliche Regelungen hat. Die Datenschutzbeauftragten von Bund und Ländern sind mit dieser Frage wiederholt unter verschiedenen Aspekten konfrontiert worden; folgende Fälle können als Beispiele angeführt werden:

Sind Amtsträger durch den Datenschutz auch davor geschützt, daß Akten in Archiven durch Bürger eingesehen werden können und daß dadurch bekannt wird, welcher Bedienstete in welcher Weise amtlich tätig geworden ist?
Sind Geschäftsverteilungspläne, Organisationspläne, Telefonlisten von Behörden grundsätzlich geheimzuhalten?
Ist es zulässig, Namensschilder von Bediensteten mit ihrer Dienst- bzw. Amtsbezeichnung an Behördentüren anzubringen?
Darf die Polizei die Anstellungsbehörde von öffentlich Bediensteten darüber unterrichten, daß diese sich möglicherweise in Ausübung ihrer Tätigkeit gegenüber der Polizei dienstpflichtwidrig verhalten haben?
Darf sich eine Behörde über Mitarbeiter einer anderen Behörde bei deren Vorgesetzten über mangelhafte Amtsausübung beschweren?

Wenn man in all diesen Fällen die Auffassung zugrunde legen würde, daß den jeweils betroffenen Bediensteten, über die Informationen übermittelt werden sollen, das informationelle Selbstbestimmungsrecht zur Seite steht und daß zudem auch zu ihren Gunsten die Übermittlungsvoraussetzungen der Datenschutzgesetze einzuhalten sind, wäre jeweils von folgender Rechtslage auszugehen:

Eine Datenübermittlung dürfte grundsätzlich nur dann erfolgen, wenn eine bereichsspezifische normenklare Rechtsgrundlage dafür vorhanden wäre. Dies ist im allgemeinen (bis auf den Archivbereich, der kürzlich gesetzlich auch bezüglich dieser Fragen normiert worden ist) nicht der Fall. § 28 BDSG dürfte als alleinige Rechtsgrundlage nicht ausreichen. Selbst wenn man dies aber akzeptieren würde, wäre in jedem Fall zu prüfen, ob die Informationsübermittlung zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist und kein Grund zur Annahme besteht, daß schutzwürdige Interessen des Betroffenen entgegenstehen (§ 28 Abs. 2 S.1 BDSG). Bei Übermittlungen über arbeitsrechtliche Rechtsverhältnisse wäre ein solches entgegenstehendes Interesse grundsätzlich zu vermuten (Arg. aus § 28 Abs. 2 S. 2 Spiegelstrich 5 BDSG). Es bliebe also nur die Möglichkeit, entsprechende Datenübermittlungen mit Einwilligung der betroffenen Bediensteten vorzunehmen. Falls diese Einwilligung nicht erteilt wird, dürften Informationsübermittlungen nicht erfolgen.

Die Unsinnigkeit dieses Ergebnisses liegt auf der Hand; es ist auch rechtlich nicht vertretbar.

Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art.1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG (so das Bundesverfassungsgericht in ständiger Rechtsprechung, zuletzt BVerfGE 78, 77/84).

Wie grundsätzlich jedes Grundrecht ist es zunächst ein Abwehrrecht der Bürger gegen den Staat. Der Staat selbst kann sich auf das informationelle Selbstbestimmungsrecht nicht berufen. Dies ist unstreitig.

Fraglich ist, ob sich ein Amtsträger als handelndes Organ des Staates in dieser Eigenschaft auf das informationelle Selbstbestimmungsrecht berufen kann, oder ob er insoweit nicht als Teil des Staates anzusehen ist und genauso wie die Organisationseinheit zu behandeln ist, der er angehört.

Letzteres läßt sich sicherlich in dieser allgemeinen Form nicht vertreten: Auch der öffentlich Bedienstete ist Grundrechtsträger gegenüber seiner Anstellungskörperschaft. Allerdings bezieht sich diese Rechtsposition als Grundrechtsträger nur auf den Bereich, in dem der öffentlich Bedienstete dem Staat als Individuum gegenübersteht, in dem er selbst dem Staat als eigenständiger Träger von Rechten und Pflichten gegenübertritt.

In dem Bereich, in dem der Amtsträger seinerseits für den Staat handelt, in dem er also Organ oder Amtswalter des Staates ist und in dem sein Handeln dem Staat zugerechnet wird, kann er schon begrifflich nicht Grundrechtsträger sein. Auch ein Blick auf den eigentlichen Inhalt des in Rede stehenden Grundrechts bestätigt dies:

Die Zubilligung des Grundrechts auf allgemeine Handlungsfreiheit und informationelle Selbstbestimmung an Amtsträger in Ausübung ihres Amtes würde bedeuten, daß der öffentlich Bedienstete bei der Ausübung seiner amtlichen Tätigkeiten gegenüber dem Bürger „seine Persönlichkeit entfaltet", „sich selbst verwirklicht", „seinen persönlichkeitsrechtlichen Freiraum wahrnimmt". Dies alles können jedoch vielleicht für den handelnden Bediensteten erfreuliche Nebenfolgen seiner amtlichen Tätigkeit sein, Hauptinhalt seiner Tätigkeit gegenüber dem Bürger muß der korrekte Aufgabenvollzug entsprechend den Gesetzen sein, der im Grundsatz von individuellen Eigenschaften des handelnden Amtsträgers unabhängig ist. Wenn aber der Inhalt des amtlichen Handelns nicht Ausdruck der individuellen Selbstbestimmung der handelnden Person ist, dann kann auch die Information über dieses Handeln nicht grundsätzlich der eigenen Dispositionsbefugnis des handelnden Amtsträgers unterliegen. Alles das, was das Bundesverfassungsgericht (im Volkszählungsurteil vom 15. Dezember 1983, BVerfGE 65, 1 ff.) zur Bedeutung des informationellen Selbstbestimmungsrechts ausgeführt hat, betrifft nicht den Amtsträger bei amtlichen Handlungen. Eine Übertragung auf diesen Bereich ist vom Grundsatz her verfehlt (so im Ergebnis auch Simitis, Stellungnahme zum Entwurf eines Bundesarchivgesetzes vom 13. September 1985, S. 11, veröffentlicht in: Veröffentlichte Gesetzesmaterialien des Parlamentsarchivs Nr. 23, Bonn 1988, S. 140; die Baden – Württembergische Landesdatenschutzbeauftragte, Dr. Leutze, spricht in ihrer Stellungnahme v. 5. September 1985, am gleichen Ort, S. 98, nur von einer „wesentlich geringeren Schutzwürdigkeit" von Amtsträgern, soweit sie in dienstlicher Funktion tätig werden). Rechtsfolge der hier vertretenen – naheliegenden – Überlegung ist demgegenüber, daß bei Informationsübermittlungen des Dienstherrn über die amtliche Funktion und Tätigkeit seiner Bediensteten keine Grundrechte der Bediensteten tangiert werden. Die Reichweite des informationellen Selbstbestimmungsrechts ist – ebenso wie die Reichweite der allgemeinen Handlungsfreiheit – im Bereich des amtlichen Handelns beschränkt, diese Grundrechte sind begrifflich auf Amtsträger in Ausübung ihrer Tätigkeit nicht anwendbar (vgl. hierzu auch den Beschluß der 3. Kammer des 1. Senats des BVerfG v. 12. April 1991, NJW 91, 2339).

Damit bleiben die Befugnisse und Aufgaben des Dienstherrn in diesem Zusammenhang nicht im rechtsfreien Raum: Sie werden jeoch nicht durch Grundrechte der Amtsträger beschränkt. Maßgeblich sind vielmehr die hergebrachten Grundsätze des Berufsbeamtentums (Art. 33 Abs. 4 GG) sowie die gesetzlichen und untergesetzlichen Ausgestaltungen des öffentlichen Dienstrechts.

Es gibt sicherlich einen weiten und bedeutsamen Bereich, in dem der öffentlich Bedienstete seinem Dienstherrn als Grundrechtsträger gegenübertritt: Dies ist insbesondere der Bereich des dienstrechtlichen Grundverhältnisses, also der gesamte Bereich, in dem der öffentlich Bedienstete nicht gegenüber dem Bürger oder gegenüber sonstigen Stellen für die Behörde nach außen handelnd tätig wird, sondern in dem er selbst als Individuum gegenüber seinem Dienstherrn berechtigt oder verpflichtet ist.

17.3.2 Schützen die Datenschutzgesetze Amtsträger vor Informationsweitergaben über amtliches Handeln?

Auch die Datenschutzgesetze haben unter dem Gesichtspunkt des Verhältnisses Bürger – Staat keinen weiteren Anwendungsbereich als den, der für das informationelle Selbstbestimmungsrecht oben dargestellt wurde. Dies ergibt sich bereits aus den jeweiligen Aufgabenbeschreibungen der Datenschutzgesetze. Zwar spricht das BDSG vom Schutz personenbezogener Daten, wobei personenbezogene Daten Einzelangaben über bestimmte oder bestimmbare natürliche Personen sind. Dem Wortlaut nach könnte als solche natürliche Person auch ein öffentlich Bediensteter anzusehen sein, der als Amtsträger handelt. Eine ähn-

liche Interpretation auf der Grundlage des Wortlauts läßt das novellierte BDSG (vom 20. Dezember 1990, BGBl. I S. 2954), das am 1. Juni 1991 in Kraft getreten ist, jedoch kaum noch zu: Danach ist Zweck des Gesetzes, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. In dieser Neufassung ist durch die Bezugnahme auf das Persönlichkeitsrecht auch die Beschränkung der Anwendung des grundrechtlichen Persönlichkeitsrechtes in Bezug genommen, die oben dargestellt wurde. Diese Formulierung des Zwecks des Datenschutzes ist in allen in der letzten Zeit novellierten Landesdatenschutzgesetzen enthalten (z. B. im hessischen, nordrhein-westfälischen, bremischen, schleswig-holsteinischen Gesetz).

Deutlicher noch kommt der Aspekt des Ziels der Datenschutzgesetze, den Bürger und nicht den Amtsträger zu schützen, im rheinland-pfälzischen LDatG sowie im hamburgischen Datenschutzgesetz (vom 31. März 1981, das in dieser Form bis zum 30. August 1990 in Kraft war) zum Ausdruck: In beiden Gesetzen ist als Aufgabe des Datenschutzes definiert, den (als Schutzobjekt ausdrücklich so benannten) Bürger vor Mißbrauch bei der Verarbeitung personenbezogener Daten zu schützen (§ 1 Abs. 1 Hamburgisches Datenschutzgesetz in der o. g. Fassung; § 1 Abs. 1 LDatG RP). Damit betreffen die datenschutzrechtlichen Übermittlungsregelungen den hier behandelten Bereich nicht.

17.3.3 Voraussetzungen von Informationsübermittlungen an Dritte

Bei der Entscheidung über Informationsübermittlungen an Dritte, die die dienstliche Tätigkeit von Amtsträgern betreffen, ist der Staat bzw. der Dienstherr dennoch nicht völlig frei; der fehlende Grundrechtsbezug der Entscheidung, soweit die Rechtssphäre der Amtsträger betroffen ist, bedeutet nicht, daß keinerlei rechtliche Vorbedingungen bzw. Schranken für die staatliche Entscheidung zu beachten wären.

Eine Informationspflicht könnte bestehen, wenn der Übermittlungsempfänger grundrechtliche oder gesetzliche Informationsansprüche geltend macht.

Zugunsten einer Geheimhaltung der begehrten Information über die Identität und den Gegenstand der Tätigkeit einzelner Amtsträger gibt es ebenfalls rechtliche Vorgaben: So ist die Funktionsfähigkeit des betroffenen Behördenapparates ein gewichtiger Gesichtspunkt, der auch auf gesetzlichen oder sogar grundgesetzlichen Entscheidungen beruht (zumindest auf der Entscheidung, eine bestimmte Behörde zu errichten, die auch grundsätzlich den gesetzgeberischen Willen – u. U. auch den Willen des Verfassungsgebers – zum Ausdruck bringt, daß eine bestimmte Behörde ihren in einem Rechtssatz fixierten Auftrag möglichst effizient zu erfüllen hat). Aber auch der Fürsorgegesichtspunkt für den Bediensteten kann zur Geheimhaltung bestimmter Informationen über bestimmte Tätigkeiten des Bediensteten zwingen oder diese Geheimhaltung zumindest nahelegen; dabei handelt es sich nicht um die Wahrung des – in diesem Zusammenhang gerade nicht heranzuziehenden – informationellen Selbstbestimmungsrechts, sondern um die Wahrung anderer Schutzgüter, beispielsweise Leben und Gesundheit der Bediensteten bei bestimmten exponierten Tätigkeiten. Auch die Frage, welchen nachgeprüften Wahrheitsgehalt eine Information besitzt, welche Richtigkeitsgewähr für sie übernommen werden kann, hat Bedeutung. Im Ergebnis muß eine Entscheidung über eine entsprechende Informationsübermittlung immer Resultat einer Rechtsgüterabwägung zwischen allen im Einzelfall bedeutsamen Faktoren sein.

In den oben genannten Beispielsfällen, die den Datenschutzbeauftragten zur Entscheidung vorgelegen haben, ist allerdings in keinem Fall ein Überwiegen des Geheimhaltungsinteresses festzustellen.

17.3.4 Datenübermittlungen an die Richterwahlausschüsse in den neuen Bundesländern

Die hier erörterte Frage hat auch in folgendem Zusammenhang für die Tätigkeit des LfD Rheinland-Pfalz Bedeutung erlangt: Zum Zweck einer Entscheidung über künftiges rechtsstaatliches Verhalten der zu überprüfenden Richter und Staatsanwälte in der ehemaligen DDR erscheint es erforderlich, die bisherige amtliche Tätigkeit dieser Staatsbediensteten, wie sie sich in Urteilen oder Anklageschriften darstellt, den zuständigen Ausschüssen zur Kenntnis zu geben. Zum einen ist es erforderlich, in diesem Zusammenhang auf die Erkenntnisquellen der zentralen Erfassungsstelle in Salzgitter zurückzugreifen, zum anderen sollten DDR-Urteile, deren Vollstreckung auf dem Gebiet der Bundesrepublik für unzulässig erklärt worden war (gem. § 15 des Gesetzes über die innerdeutsche Rechts- und Amtshilfe in Strafsachen) auch durch rheinland-pfälzische Behörden (Generalstaatsanwälte) an die genannten Ausschüsse übersandt werden.

Im Fall der Salzgitter-Unterlagen hat man den Weg gewählt, die zu überprüfenden Bediensteten um ihre Einwilligung zu ersuchen. Aus einer verweigerten Einwilligung sollten dann negative Folgerungen bezüglich der Weiterbeschäftigung gezogen werden können (so die Entscheidung des Bundesministers der Justiz aufgrund des durch entsprechende Datenübermittlungen angeblich eingeschränkten Rechts auf informationelle Selbstbestimmung der betroffenen Richter und Staatsanwälte, vgl. Beitrag „Zu prüfende Prüfer" in der FAZ Nr. 267 vom 15. November 1990).

Bezüglich der Nichtvollstreckungsentscheidungen hat man § 6 Abs. 3 i. V. m. § 10 Abs. 3 Satz 3 der „Ordnung für die Bildung

und Arbeitsweise der Richterwahlausschüsse" eine gesetzliche Grundlage entnommen. Die genannte Rechtsvorschrift enthält aber für die in Rede stehenden Datenübermittlungen gerade keine ausdrückliche Grundlage, die den verfassungsrechtlichen Anforderungen an ein grundrechtseinschränkendes Gesetz genügen würde.

Auf der Basis der oben dargestellten Überlegungen ist jedoch weder eine Einwilligung der betroffenen Bediensteten noch eine ausdrückliche gesetzliche Grundlage, die den Anforderungen des Bundesverfassungsgerichts an eine Eingriffsermächtigung in das informationelle Selbstbestimmungsrecht genügen müßte, Voraussetzung zulässiger Datenübermittlungen. Der allgemeine Rechts- und Amtshilfegrundsatz reicht als Rechtsgrundlage aus, da mit der Übermittlung nicht in Grundrechtspositionen der betroffenen Richter und Staatsanwälte eingegriffen wird.

17.3.5 Sonstige Auskunftsersuchen über Amtsträger

Auch in einer Reihe von Eingaben und Anfragen an die DSK ging es um die oben dargestellte Grundsatzfrage, ob Amtsträger im Rahmen der Wahrnehmung ihrer amtlichen Aufgaben Betroffene im Sinne datenschutzrechtlicher Vorschriften sind. Diese Frage stellte sich beispielsweise bei der Weigerung einer Bezirksregierung, einem Interessenten die Namen und Anschriften der Mitglieder des Beirates für Landespflege mitzuteilen. Begründet wurde dies mit dem Hinweis, die Weitergabe der personenbezogenen Daten sei nur mit Zustimmung der Betroffenen zulässig.

Entsprechend der oben wiedergegebenen Grundsätze waren gegen die Bekanntgabe der Mitglieder des Beirates für Landespflege keine datenschutzrechtlichen Bedenken zu erheben.

In einem Wahlanfechtungsverfahren wollte die Klägerin von einer Stadtverwaltung wissen, in welchen Wahlbezirken konkret benannte Personen dem Wahlvorstand angehörten und von welchen Parteien sie vorgeschlagen wurden. Auch in diesem Falle wurde der obige Rechtsstandpunkt vertreten. Ergänzend wurde darauf hingewiesen, daß angesichts eines qualifizierten, auf die Gewinnung zusätzlicher Erkenntnisse für einen anhängigen Verwaltungsrechtsstreit gerichteten Interesses kein Grund bestehe, der Klägerin die Namen und Adressen von Wahlvorstandsmitgliedern vorzuenthalten. Hingegen – so die Auffassung der DSK – berühre die Auskunft, von welchen Parteien Wahlvorstandsmitglieder vorgeschlagen wurden, nicht nur die für das amtliche Handeln bedeutsamen Informationen, sondern auch den eher persönlichkeitsbezogenen Bereich der politischen Überzeugung. Informationen über eine Parteimitgliedschaft dürften – jedenfalls bei einfachen Parteimitgliedern – dem informationellen Selbstbestimmungsrecht unterliegen. Eine Partei wird zwar von der mutmaßlichen Zustimmung der Betroffenen in die Datenübermittlung an die Gemeinde ausgehen können. Diese Zustimmung richtet sich indessen nur darauf, daß die Gemeinde den Vorschlag zur Kenntnis erhält. Eine weitere Offenbarung durch diese bedürfte als Informationseingriff – von Zustimmungsfällen abgesehen – der gesetzlichen Legitimierung. Keine Bedenken bestünden gegen anonymisierte Auskünfte dergestalt, daß dem Fragesteller mitgeteilt wird, wie viele Mitglieder eines Wahlvorstands von welcher Partei vorgeschlagen wurden.

17.4 Pflicht zur Verfassungstreue im öffentlichen Dienst

Als Konsequenz der politischen Veränderungen im ehemaligen Ostblock, insbesondere der Wiedervereinigung Deutschlands, wurden die verwaltungsinternen Reglungen über die Überprüfung von Bewerbern für den öffentlichen Dienst mit Beteiligung der DSK im Dezember 1990 geändert. Aufgrund der Verwaltungsvorschrift des Ministeriums des Innern vom 27. Dezember 1990 „Pflicht zur Verfassungstreue im öffentlichen Dienst" (MinBl. 91 S. 15 – im amtlichen Gültigkeitsverzeichnis 1991 nicht verzeichnet –) ist die sog. Regelanfrage entfallen. Jeder Bewerber ist vor der Entscheidung über die Einstellung über seine Pflicht zur Verfassungstreue in geeigneter Form schriftlich zu belehren. Bei der Einstellung von Beamten sowie von Angestellten und Arbeitern, denen dauerhaft hoheitliche Aufgaben übertragen werden sollen, ist die Einstellungsbehörde verpflichtet, die Verfassungstreue selbst im Vorstellungsgespräch oder aufgrund schriftlicher Personalunterlagen festzustellen. Nur noch dann, wenn die Verfassungstreue des Bewerbers auf diese Weise nicht zweifelsfrei festgestellt werden kann, erfolgt eine Anfrage beim Ministerium des Innern und für Sport.

Diese Regelung wird zur Zeit auch noch auf Bewerber aus den neuen Bundesländern angewendet. Um den Einstellungsbehörden nähere Anhaltspunkte für die Überprüfungen zu geben, wurden erläuternde Rundschreiben des Bundesministers des Innern (zuletzt vom 26. Februar 1991) zur Information versandt, die in den Anlagen u. a. Listen der wichtigsten „Massenorganisationen" und „Gesellschaftlichen Organisationen" sowie ein Aufbauschema der SED der ehemaligen DDR enthalten.

In der Praxis können bei konkreten Anhaltspunkten für eine Tätigkeit im ehemaligen Staatssicherheitsdienst Anfragen an den Sonderbevollmächtigten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes nach Maßgabe der vorläufigen Ordnung für deren Nutzung gerichtet werden.

Nunmehr besteht die Absicht, die o. g. Verwaltungsvorschrift im Blick auf Bewerber aus dem Beitrittsgebiet bereichsspezifisch zu ergänzen. Ein entsprechender Entwurf ist dem LfD zur Stellungnahme zugeleitet worden. Ihm liegt – wie auch der bisherigen Praxis – die Feststellung zugrunde, daß bei Bewerbern aus den neuen Bundesländern die Verfassungstreue auch von deren

früherem Verhalten im Gefüge der ehemaligen DDR abhängt. Hierfür werden zunächst Konkretisierungen vorgenommen, die sich auf Verstöße gegen die Grundsätze der Menschlichkeit und der Rechtsstaatlichkeit sowie auf näher bezeichnete Tätigkeiten und Funktionen insbesondere im Ministerium für Staatssicherheit/Amt für Nationale Sicherheit der DDR sowie in der SED und den Blockparteien beziehen.

Das vorgesehene Verfahren sieht im wesentlichen ein hierüber zu führendes Gespräch mit dem Bewerber vor und bei Vorliegen entsprechender Anhaltspunkte eine Anfrage beim Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes. Hierfür ist die Zustimmung des Bewerbers erforderlich.

So ähnelt das Verfahren in seiner Struktur weitgehend der Prüfung, wie sie in der schon in Kraft befindlichen Verwaltungsvorschrift für alle Bewerber des öffentlichen Dienstes vorgesehen ist. Damit stellt sich zwar die Frage, ob – wie bereits in anderen Ländern – von einer gesonderten Regelung für Bewerber aus den neuen Bundesländern überhaupt abgesehen werden sollte. Hierfür spräche sowohl, daß man in der Sonderregelung möglicherweise eine Diskriminierung sehen könnte, wie auch die vermutlich geringe Zahl der Bewerber. Andererseits ist nicht zu verkennen, daß eine bereichsspezifische Regelung gerade hier der Rechtsklarheit dient, eine einheitliche Praxis sicherstellt und ungeregelte Nachforschungen verhindert. Die letztgenannten Überlegungen liegen auch im Interesse der Betroffenen. Damit ist der bereichsspezifischen Ergänzung der Verwaltungsvorschrift letztlich auch aus der Sicht des Datenschutzes der Vorzug zu geben.

Zum Entwurf selbst sind folgende Überlegungen zu berücksichtigen:

Die vorgesehene Würdigung des „persönlichen Verhaltens vor und nach der Wiedervereinigung" darf nicht zu einer umfassenden Ausforschung der persönlichen Verhältnisse des Bewerbers führen. Feststellungen dieser Art müssen deshalb streng zweckorientiert bleiben und dürfen keinesfalls über das hinausgehen, was an Fakten für die Feststellung der Verfassungstreue unerläßlich ist. Dies wäre durch eine ergänzende Klarstellung in geeigneter Weise sicherzustellen.

Auf jeden Fall müßte in hervorgehobener Form – ggf. durch eine eigene Ziffer – die strikte Beachtung des Grundsatzes der Verhältnismäßigkeit in diesem die Betroffenen besonders belastenden Verfahren ausdrücklich angeordnet werden.

Es sollte geprüft werden, ob bei Bewerbern für einen Vorbereitungsdienst, der Voraussetzung für die Ausübung eines Berufes auch außerhalb des öffentlichen Dienstes ist (z. B. Juristenausbildung), auf die Anfrage beim Sonderbeauftragten verzichtet werden kann. In der Verwaltungsvorschrift ist auf alle Fälle zu bestimmen, daß Anfragen nur dann erfolgen, wenn eine Einstellung tatsächlich beabsichtigt ist.

In dem Entwurf der Verwaltungsvorschrift ist eine Anfrage beim Sonderbeauftragten u. a. vorgesehen, wenn nach dem Prüfungsgespräch Anhaltspunkte für die Wahrnehmung einer Tätigkeit für den Staatssicherheitsdienst vorliegen. Hier sollten „tatsächliche Anhaltspunkte" zur Voraussetzung gemacht werden.

Die in § 17 Abs. 1 Satz 6 der Vorläufigen Ordnung für die Nutzung personenbezogener Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amt für Nationale Sicherheit vorgesehene Möglichkeit, in einem Ersuchen die Daten mehrerer zu überprüfender Personen in einer Liste aufzuführen, ist bei Personaleinstellungsverfahren datenschutzrechtlich bedenklich. Es müßte daher in der Verwaltungsvorschrift die Einzelanfrage vorgeschrieben werden.

Dem Bewerber sollte in der Verwaltungsvorschrift die Möglichkeit eingeräumt werden, beim Rücklauf der Auskunft des Sonderbeauftragten deren Inhalt zunächst einmal ausschließlich selbst zur Kenntnis zu nehmen. Das in § 30 Abs. 5 des Bundeszentralregistergesetzes vorgeschriebene Verfahren für die Vorlage von Führungszeugnissen bei Behörden könnte hierfür im Grundsatz übernommen werden.

In dem Entwurf fehlen schließlich den Anforderungen des Datenschutzes genügende Bestimmungen über die Aufbewahrung und Löschung der bei der Überprüfung erhobenen Daten. Es müßte vorgesehen werden, daß jedenfalls die Niederschrift über das Bewerbungsgespräch und evtl. Erkenntnisse des Sonderbeauftragten nur in verschlossenem Umschlag zu den Personalakten genommen werden. Bezüglich der Vernichtung von Unterlagen über erfolglos gebliebene Bewerber wäre auf die hierfür einschlägige Verwaltungsvorschrift ausdrücklich hinzuweisen.

17.5 Personalinformationssysteme

Die Frage der Zulässigkeit von Datenspeicherungen öffentlich Bediensteter und der Mitbestimmungspflicht automatisierter Personaldatenverarbeitungssysteme ist insbesondere im Schulbereich problematisiert worden. Auf Fragen von Lehrern und Schulen, ob die automatisierte Erfassung von Lehrerdaten auf der Ebene der Schule zulässig sei und ob dies der Mitbestimmung unterliege, hat der LfD wie folgt geantwortet:
Zunächst ist darauf hinzuweisen, daß die Speicherung des Bekenntnisses in schulischen Personalverwaltungssystemen grund-

sätzlich nicht zulässig ist. Zur Erfüllung der schulbezogenen gesetzlichen Aufgaben ist zwar möglicherweise die Kenntnis erforderlich, ob ein Lehrer bereit ist, Religionsunterricht zu erteilen und in welchem Bekenntnis dies erfolgen könnte. Welche Religionszugehörigkeit der Lehrer selbst besitzt, ist jedoch eine hiervon zu unterscheidende Information, für deren Speicherung auf der Ebene der Schule grundsätzlich kein Erfordernis besteht.

Zur Frage der Mitbestimmungspflicht hat der LfD nur insoweit Stellung genommen, als Mitbestimmungstatbestände in Betracht kommen, die auch der Sicherung des informationellen Selbstbestimmungsrechts der Betroffenen dienen. Hier ist in erster Linie die Regelung des § 77 a Abs. 1 Nr. 5 Landespersonalvertretungsgesetz zu nennen, wonach Personalinformationssysteme der Mitbestimmungspflicht unterliegen.

Der Begriff des Personalinformationssystems ist durch das Gesetz selbst nicht definiert. Eine an Sinn und Zweck sowie der Entstehungsgeschichte und der systematischen Stellung der Norm orientierte Auslegung ergibt, daß hierunter diejenigen Systeme der Personaldatenverarbeitung zu verstehen sind, die

- Informationen über konkrete Leistungen der Bediensteten oder Beurteilungsmerkmale bzw. Angaben über die Art der Aufgabenerfüllung oder die Qualifikation enthalten und

- die zu allgemeinen Personaleinsatzplanungs- bzw. allgemeinen Personalverwaltungszwecken vorgehalten werden.

Nur in derartigen Fällen liegt nach Auffassung des LfD ein Personalinformationssystem vor.

Unabhängig vom Inhalt der automatisiert gespeicherten Daten ist unter dem Aspekt des Schutzes der den PC konkret bedienenden Beschäftigten ergänzend auf die Regelung des § 77 a Abs. 1 Nr. 2 LPersVG hinzuweisen, wonach Einrichtungen mitbestimmungspflichtig sind, die geeignet sind, die Leistung oder das Verhalten von Bediensteten zu überwachen.

Geräte mit dem Betriebssystem MS-DOS sind grundsätzlich zu einer solchen Überwachung des Bedienungspersonals geeignet, vgl. das Urteil des VGH Kassel vom 8. August 1990, Az. BPVTK 557/90.

Aus datenschutzrechtlicher Sicht bestehen keine Bedenken dagegen, daß die Zentrale Besoldungs- und Versorgungsstelle bei der OFD Koblenz, die für die Besoldung der Landesbediensteten zuständig ist, im Auftrag der Dienststelle, die ein Personalinformationssystem betreibt, auf Speichermedien der automatisierten Datenverarbeitung die Daten zum Zweck des Systemaufbaus übermittelt, die dazu erforderlich und Teil der in der Dienststelle vorhandenen Personalakten sind. Soweit dies der Fall ist, liegt keine Offenbarung von Daten bzw. Informationen vor. Bedenken gegen die technische Erleichterung bei der automatisierten Erfassung dieser Daten ergeben sich aus datenschutzrechtlicher Sicht nicht.

17.6 Zeiterfassungs- und Zugangskontrollsysteme

Die DSK hat den Entwurf einer Dienstvereinbarung über die Einführung und Nutzung von Zugangskontrollsystemen im Bereich einer großen Universität des Landes überprüft.

Sie konnte aus datenschutzrechtlicher Sicht keine Regelungen erkennen, die die datenschutzrechtlichen Belange der Bediensteten unangemessen oder rechtswidrig beeinträchtigen würden. Auch entsprechende Regelungsdefizite waren nicht ersichtlich.

Es war nicht ihre Aufgabe, zu dem Bereich Stellung zu nehmen, der die Befugnisse des Personalrats gegenüber der Dienststelle betrifft. Diesbezüglich hat sie sich einer inhaltlichen Bewertung enthalten.

17.7 Leistungserfassung durch statistische Aufzeichnungen

Es war zu beurteilen, ob eine permanente Leistungskontrolle in Form der Statistik der Medizinischen Dienste der Krankenversicherung unter dem Gesichtspunkt des Personaldatenschutzes grundsätzlich unzulässig und inwieweit die Einführung einer solchen Datenerfassung mitbestimmungspflichtig ist.

Die Statistik des Medizinischen Dienstes enthält beispielsweise folgende Angaben zur Arbeitsleistung der betroffenen Mediziner:

Angaben zum Begutachtungsfall: Geburtsdatum des Begutachteten; Geschlecht; Mitgliedsgruppe; Gutachtenart; arbeitsunfähig seit; Auftrag der Kasse; Auskunft des Behandlers; den Gutachtungsanlaß; Grundlage; Stellungnahme zur Arbeitsunfähigkeit; Übereinstimmung mit dem Behandler; Stellungnahme zu besonderem Anlaß; Hinweis auf besondere Ursachen; Empfehlung an Kasse; Empfehlung an Behandler; Empfehlung an Versicherten.

Dabei ist zu den einzelnen Merkmalen jeweils wohl nur eine Ja/Nein-Alternative bzw. die Eintragung einer einstelligen (nur beim Begutachtungsanlaß zweistelligen) Schlüsselziffer möglich.

a) Zur Frage, ob eine permanente Leistungskontrolle in Form der beschriebenen Informationserhebung und -speicherung zulässig ist:

Eine entsprechende Datenerhebung wäre unzulässig, wenn sie ohne ausreichende Rechtsgrundlage erfolgen oder gegen ausdrückliche gesetzliche Regelungen verstoßen würde. Rechtsgrundlage für die Datenerhebung ist das aus dem Arbeits- bzw. Dienstverhältnis mit den betroffenen Ärzten abzuleitende Direktionsrecht des Dienstvorgesetzten. Eine Grenze liegt in der schrankenlosen Erfassung der Persönlichkeit des Arbeitnehmers. Dies würde in den Kernbereich der Persönlichkeitsrechte eingreifen und auch das informationelle Selbstbestimmungsrecht im Kernbereich beeinträchtigen. Eine solche umfassende Verhaltenserfassung ist jedoch mit den beschriebenen Aufzeichnungen nicht verbunden: Es wird der Tagesablauf der einzelnen Bediensteten nicht lückenlos erfaßt. Eine lückenlose Erfassung der konkreten Arbeitsleistung in ihren Ergebnissen ist jedoch grundsätzlich zulässig; dadurch wird nicht in den Kernbereich der genannten Grundrechte eingegriffen. Diese Erfassung muß dem Arbeitgeber grundsätzlich möglich sein, schon um die anfallende Arbeit sachgerecht und leistungsgerecht verteilen zu können. Es ist grundlegende Voraussetzung der Ausübung von Dienstaufsicht, die Arbeitsergebnisse der einzelnen Mitarbeiter lückenlos zu kennen und ggf. auch zu dokumentieren. Unzulässig wäre dagegen beispielsweise die lückenlose Erfassung des Verhaltens der Bediensteten. Eine solche Erfassung ist jedoch nicht erfolgt.

b) Zur Frage der Mitbestimmungspflicht:

Bei einer automatisierten Speicherung entsprechender Angaben zu jedem einzelnen Arzt und zu jeder einzelnen Beratung oder jedem einzelnen Begutachtungsfall würde es sich um ein Personalinformationssystem handeln, für das eine Mitbestimmungspflicht gemäß § 77 a Abs. 1 Nr. 5 Personalvertretungsgesetz bestünde.

Wenn diese Angaben jedoch nur in Karteiform vorliegen, kann von einem Personalinformationssystem nicht gesprochen werden. Es käme dann als Mitbestimmungstatbestand § 77 a Abs. 1 Nr. 1 in Betracht: Hierbei könnte es sich um eine Maßnahme zur Hebung der Arbeitsleistung handeln. Die Aufzeichnungspflicht bezüglich jedes Arbeitsergebnisses dürfte unter diese Alternative fallen. Damit wäre die Einführung einer solchen arbeitsleistungsbezogenen Aufzeichnung grundsätzlich mitbestimmungspflichtig. Der LfD ist für die Beurteilung dieser Frage jedoch nicht zuständig: Der Mitbestimmungstatbestand des § 77 a Abs. 1 Nr. 1 dient nicht dem Schutz der Bediensteten vor Eingriffen in ihr informationelles Selbstbestimmungsrecht; Zweck des Mitbestimmungstatbestandes ist vielmehr die Wahrung des allgemeinen Selbstbestimmungsrechts sowie der allgemeinen Handlungsfreiheit auch im Betrieb.

Als technische Einrichtung, die geeignet ist, die Leistung der Mitarbeiter zu überwachen (dies würde eine Mitbestimmungspflicht gem. § 77 a Abs. 1 Nr. 2 LPersVG auslösen), ist das vorliegende Datenerfassungssystem deshalb nicht anzusehen, weil durch die EDV keine unmittelbare Erfassung von Leistungs- oder Verhaltensinformationen erfolgt, diese Daten vielmehr manuell erhoben und erst anschließend automatisiert verarbeitet werden.

Als weiterer Mitbestimmungstatbestand käme auch § 77 Nr. 15 (Ausgestaltung von Personalfragebogen) in Betracht. Hierbei handelt es sich jedoch nur um Zusammenstellungen von Fragen, die Aufschluß über die Person, Kenntnisse und Fertigkeiten des Befragten geben sollen. Die Aufzeichnung von Arbeitsergebnissen unterliegt diesem Begriff nicht (vgl. zur Definition des Begriffs Fitting/Auffarth/Kaiser/ Heither, Randziffer 2 zu § 94 Betriebsverfassungsgesetz).

Danach ist als Ergebnis festzuhalten, daß die beschriebene Leistungsdatenerfassung grundsätzlich zulässig ist und daß in diesem Zusammenhang kein spezifisches Mitbestimmungsrecht zur Wahrung datenschutzrechtlicher Belange besteht.

17.8 Telefondatenerfassung

Die DSK hat ihre bereits im 8. Tätigkeitsbericht (Tz. 5.5) dargelegte Auffassung, daß es grundsätzlich unzulässig ist, die Zielnummer privater Telefonate durch den Dienstherrn mit allen Ziffern zu speichern, in wiederholten Anworten auf konkrete Anfragen bestätigt.

Sie hat ihre Auffassung ebenfalls aufrechterhalten, wonach es grundsätzlich zulässig ist, die Gesprächsdaten dienstlicher Telefonate auch unter Angabe der Zielnummer aufzuzeichnen.

Im Berichtszeitraum hatte sie zu beurteilen, ob es zulässig war, daß der Rechnungshof bzw. ein Gemeindeprüfungsamt die aufgezeichneten Telefondaten zur Überprüfung nutzte, ob tatsächlich die als dienstlich bezeichneten Telefonate auch dienstlichen Zwecken gedient haben. Die DSK hat keine Bedenken dagegen gehabt, daß das Gemeindeprüfungsamt entsprechende Unterlagen in personenbeziehbarer Form erhält. Die entsprechenden Rechtsgrundlagen finden sich in § 14 RHG i. V. m. § 110 Abs. 4 GemO sowie § 95 LHO. Aus dem Inhalt dieser Unterlagen können Folgerungen bezüglich der wirtschaftlichen und sparsamen Haushaltsführung gezogen werden. Eine Verpflichtung zur Vorlage einer etwa vorhandenen besonderen Liste privater Telefonate, deren Gebühren der Gemeindekasse erstattet worden sind, in personenbeziehbarer Form gegenüber dem Rechnungshof

besteht allerdings nicht. Eine solche Liste könnte grundsätzlich für die Erfüllung des Prüfungsauftrags nicht erforderlich sein. Die DSK hat ergänzend betont, daß eine Verpflichtung des Gemeindeprüfungsamtes besteht, bei der Darstellung von Vorgängen in Prüfungsberichten die Persönlichkeitsrechte Dritter zu wahren.

17.9 Beihilfe

Im Bereich der Beihilfegewährung sind aus datenschutzrechtlicher Sicht einige Fragen nach wie vor noch nicht, jedenfalls noch nicht in vollem Umfang, zufriedenstellend gelöst.

17.9.1 Abschottung der Beihilfestellen von den jeweiligen Personalabteilungen

Zum Problem der Abschottung der Beihilfestellen gegenüber den Personalabteilungen hat die DSK bereits deutlich Stellung genommen (12. Tb, Anlage 6, III.2, S. 108; 12.Tb, Tz. 15.4.1, S. 79). Eine gesetzliche Regelung dazu besteht jedoch nach wie vor nicht. Es ist fraglich, wann mit der Verabschiedung der diesbezüglichen Bestimmung (vgl. Entwurf zu § 56 a Satz 3 Beamtenrechtsrahmengesetz, Gesetzentwurf der Bundesregierung vom 13. Juni 1990, Bundestagsdrucksache 11/7390 neu S. 8) zu rechnen ist. Der LfD hat das zuständige Ministerium gebeten zu prüfen, ob die Umsetzung einer entsprechenden Regelung in das Landesrecht nicht bereits im Vorgriff auf die zu erwartende bundesrechtliche Rahmenvorschrift möglich wäre. Dies ist bislang – insbesondere im Hinblick auf die in naher Zukunft erwartete Verabschiedung des genannten Bundesgesetzes – abgelehnt worden.

17.9.2 Datenübermittlungen und zentrale Erfassung von Beihilfeanträgen in Fällen nicht rechtswidrigen Schwangerschaftsabbruchs und nicht rechtswidriger Sterilisation beim Ministerium der Finanzen

Es dürfte weithin unbekannt sein, daß Beihilfeansprüche grundsätzlich auch für nicht rechtswidrige Schwangerschaftsabbrüche und für Sterilisationen bestehen (§ 92 LBG), und daß alle derartigen Anträge von Landesbediensteten (und grundsätzlich auch die aller kommunalen Bediensteten) zentral beim Ministerium der Finanzen bearbeitet und aufbewahrt wurden. Dafür existiert keine Rechtsgrundlage. Bereits die DSK hat das Ministerium wiederholt darauf hingewiesen und um eine Änderung dieses Verfahrens ersucht; zumindest wäre eine normenklare Rechtsgrundlage zu schaffen, die den Betroffenen deutlich macht, welche Stellen von ihren diesbezüglichen Beihilfeanträgen Kenntnis erhalten. Das Finanzministerium hat zugesichert, eine entsprechende RVO zu erlassen. Die in der Vergangenheit gesammelten Unterlagen sind inzwischen nach Auskunft des Ministeriums vernichtet worden.

17.9.3 Beihilfe für Angehörige

Aus Eingaben ergibt sich, daß es volljährige Kinder von Beihilfeberechtigten oder getrennt lebende Ehegatten als schwer hinnehmbar empfinden, wenn sie ärztliche Diagnosen und Arztbesuche dem Beihilfeberechtigten offenbaren müssen, der dann die entsprechenden Unterlagen an die Beihilfestelle weitergibt. Die DSK und der LfD haben sich – bislang jedoch ohne Erfolg – in diesem Zusammenhang für eine schonendere Verfahrensweise eingesetzt. In der Frage der Möglichkeiten für Angehörige von Beihilfeberechtigten, den Beihilfeanspruch unter Beachtung ihres informationellen Selbstbestimmungsrechtes zu realisieren, wurde das Ministerium der Finanzen wiederholt um Prüfung gebeten.

Die grundsätzlich wirksamste Lösung des Problems würde darin bestehen, volljährigen Angehörigen des Beihilfeberechtigten einen unmittelbaren Beihilfeanspruch gesetzlich zuzubilligen. Dies ist aus rechtssystematischen Gründen aber schwierig. Auf der Grundlage des geltenden Rechts könnte auf der Ebene der Verwaltung jedoch folgendes Verfahren für eine Verbesserung des derzeitigen Zustandes eingeführt werden:

Die Familienangehörigen, die ärztliche Rechnungen mit Diagnoseangaben dem Beihilfeberechtigten unmittelbar nicht zur Kenntnis geben wollen, sollten ihre Unterlagen direkt der Beihilfestelle zuleiten können, während der Beihilfeberechtigte im Antragsformular hierauf lediglich Bezug zu nehmen braucht. Ebenso sollten die Rechnungen mit den Diagnoseangaben in diesen Fällen von der Beihilfestelle unmittelbar an die betroffenen Angehörigen zurückgesandt werden.

Diese Verfahrensweise ist – wie sich auch aus der Stellungnahme der Bundesregierung zum 12. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz ergibt – vom Bundesminister des Innern akzeptiert. Inwieweit im Bundesbereich bereits tatsächlich entsprechend verfahren wird, ist nicht bekannt; die Bereitschaft des Bundesministers des Innern, eine entsprechende Regelung zu erlassen, liegt offensichtlich vor.

Vor diesem Hintergrund sollte es ermöglicht werden, im Bereich des Landes Rheinland-Pfalz entsprechend zu verfahren. Praktische Schwierigkeiten dürften dadurch, wie zwischenzeitliche Gespräche mit Mitarbeitern von Beihilfestellen ergeben haben, nicht entstehen: Wenn Leistungen erstattet werden – was die Regel ist – ergeben sich keine Probleme. In den relativ seltenen Fällen der Nichterstattung gerade solcher Leistungen, die in Rede stehen, könnte nach einem Hinweis an den betroffenen Ange-

hörigen die Angelegenheit gegenüber dem Beihilfeberechtigten in vollem Umfang erörtert werden. Die überwiegende Zahl der problematischen Fälle wäre damit jedoch datenschutzgerecht gelöst. Das Ministerium der Finanzen hat die Bereitschaft erkennen lassen, dem datenschutzrechtlichen Anliegen entgegenzukommen, und will sich in den länderübergreifenden Beratungen für eine solche Lösung einsetzen.

17.9.4 Rechnungsprüfung und Beihilfedaten

Anlaß der Befassung der DSK mit diesem Problem war ein Fall in einer Verbandsgemeinde. Das Gemeindeprüfungsamt hatte dort festgestellt, daß dem Bürgermeister zu Unrecht Beihilfeleistungen in Höhe von ca. 16 000 DM ausbezahlt worden waren. Außerdem wurde festgestellt, daß der Bürgermeister in ca. 20 Fällen Fahrtkostenerstattungen für Fahrten erhalten hat, die ein anderer Gemeindebediensteter abgerechnet hat.

Fraglich ist, ob der Gemeinderat über den Inhalt dieser Prüfungsfeststellungen in einer Form informiert werden muß oder darf, die Rückschlüsse auf den Nutznießer der Überzahlungen zuläßt.

§ 33 Abs. 1 Gemeindeordnung bestimmt:

„Der Gemeinderat ist vom Bürgermeister über alle wichtigen Angelegenheiten in der Gemeinde, insbesondere über das Ergebnis überörtlicher Prüfungen zu unterrichten."

Die Verwaltungsvorschrift zu § 33 Gemeindeordnung konkretisiert dies wie folgt:

„Die Verpflichtung des Bürgermeisters, den Gemeinderat über das Ergebnis der Prüfung durch das Gemeindeprüfungsamt bzw. den Rechnungshof zu unterrichten, betrifft nicht nur die Zusammenfassung des Prüfungsergebnisses, sondern auch alle Einzelfeststellungen der Prüfungsmitteilungen, die die Aufgaben des Gemeinderats (§ 32), insbesondere die Gestaltung des Haushaltsplans betreffen. Zur Vorbereitung der Beratungen im Gemeinderat hat der Bürgermeister einem Vertreter jeder Ratsfraktion den gesamten Prüfungsbericht sowie eine etwaige Stellungnahme der Verwaltung zu einzelnen Prüfungsfeststellungen zu überlassen."

Der Inhalt dieser Regelungen ist eindeutig: Im vorliegenden Fall wäre der gesamte Prüfungsbericht jeweils einem Vertreter jeder Ratsfraktion auszuhändigen.

Fraglich war, ob dieses Ergebnis unter verfassungsrechtlichen Gesichtspunkten des Datenschutzes zu modifizieren ist.

a) Eine Änderung der in Rede stehenden Verwaltungsvorschrift wäre dann zu fordern, wenn das informationelle Selbstbestimmungsrecht von Betroffenen zwingend eine Beschränkung der Unterrichtung des Gemeinderats und der Vertreter der Ratsfraktionen erfordern würden, die etwa zum Gegenstand hätte, Prüfungsfeststellungen zu anonymisieren.

   Dies ist nicht der Fall: Soweit es sich bei den Prüfungsfeststellungen um Angaben über dienstliche Tätigkeiten von einzelnen Bediensteten handelt, greift das informationelle Selbstbestimmungsrecht nicht ein, denn hier hat der Bedienstete als Amtsträger nach außen hin gehandelt. Für derartige Handlungen kann er sich nicht auf das Individualrecht berufen, selbst bestimmen zu können, wer darüber etwas erfährt. In diesen Bereich dürfte der Komplex Dienstreisen sowie dienstliche Telefonate fallen.

   Der Komplex Beihilfenerstattung ist grundsätzlich vom informationellen Selbstbestimmungsrecht des Bediensteten umfaßt, da es sich hierbei um Abrechnungsvorgänge handelt, die ausschließlich das Verhältnis des Dienstherrn zu seinem Bediensteten betreffen. Insofern ist hier für Eingriffe in dieses Recht der Verhältnismäßigkeitsgrundsatz, insbesondere auch in Gestalt des Erforderlichkeitsgrundsatzes, zu beachten. Auch unter Zugrundelegung dieses Maßstabs ergibt sich jedoch nicht, daß es unverhältnismäßig wäre, den Gemeinderat über unberechtigte Auszahlungen in Höhe von 16 000 DM an den Verbandsgemeindebürgermeister zu unterrichten. Hier handelt es sich vielmehr um Vorgänge, die die Haushaltsführung unmittelbar betreffen und die so gewichtig sind, daß sie zu Folgerungen im Entlastungsverfahren führen können (§ 32 Nr. 3 Gemeindeordnung). Bedeutsam ist auch, daß der Bürgermeister als Repräsentant der Gemeindeverwaltung in besonderem Maße einer Kontrolle durch den Gemeinderat unterliegt. Eine Berufung auf das informationelle Selbstbestimmungsrecht des Bürgermeisters gegenüber dem Gemeinderat bezüglich seines Dienstverhältnisses dürfte nur in seltenen Ausnahmefällen in Betracht kommen. § 33 Gemeindeordnung ist schließlich ausreichend normenklar, um entsprechende Datenübermittlungen zu rechtfertigen.

Im Ergebnis ist aus dem informationellen Selbstbestimmungsrecht der Bediensteten weder eine Pflicht noch eine Befugnis des Gemeindevorstands abzuleiten, den Prüfungsbericht zurückzuhalten oder inhaltlich zu verändern.

b) Ein angemessener Schutz des informationellen Selbstbestimmungsrechts der Bediensteten in diesem Zusammenhang ist allerdings durch Beachtung folgender Maßgaben sicherzustellen:

- Bereits der Bericht des Rechnungsprüfungsamtes ist grundsätzlich im Hinblick darauf zu formulieren, daß er (zwangsläufig) einem größeren Kreis von Empfängern zugeht. Der allgemeine Verhältnismäßigkeitsgrundsatz erfordert also, betroffene Bedienstete nur dann zu benennen, wenn dies unabdingbar ist und ansonsten weitgehend zu anonymisieren. Zu erwähnen ist auch die vom Rechnungshof praktizierte Verfahrensweise, Einzelpersonen mit Nummern zu bezeichnen und eine Referenzliste zu führen, die grundsätzlich nicht an Dritte übermittelt wird. Allerdings folgt aus dieser Verpflichtung der rechnungsprüfenden Stellen kein Recht des Bürgermeisters, in eigener Verantwortung nun seiner Ansicht nach erforderliche Anonymisierungen im Wege einer Art von Ersatzvornahme durchzuführen. Diese Verpflichtung obliegt vielmehr ausschließlich den berichterstellenden Stellen und ist in deren eigener Verantwortung zu beachten. Allerdings steht dem Bürgermeister das Recht zu, die berichterstattende Stelle darauf aufmerksam zu machen, wenn seiner Ansicht nach eine der o. g. Obliegenheiten nicht beachtet wurde. Dieses Recht führt jedoch nicht zu einer Verlagerung der gesetzlichen Handlungskompetenzen; es ist vielmehr – vergleichbar der beamtenrechtlichen Remonstration – als bloßes Hinweisrecht aufzufassen.

  Im vorliegenden Fall bestanden aus datenschutzrechtlicher Sicht keine Bedenken gegen die Namhaftmachung des Bürgermeisters im Bericht.

- Die Erörterung des Prüfungsberichts im Gemeinderat hat allerdings dann in nichtöffentlicher Sitzung zu erfolgen, wenn Angelegenheiten erörtert werden, die unmittelbaren Bezug zu bestimmten namhaft gemachten oder identifizierbaren Bediensteten besitzen. Dies ergibt sich aus § 35 Abs. 1 Satz 1 Gemeindeordnung sowie aus dem Rechtsgedanken des § 33 Abs. 2 Gemeindeordnung (vgl. Nr. 2 der Verwaltungsvorschrift zu § 20 Gemeindeordnung).

17.10 Datenübermittlungen durch den Arbeitgeber an Versicherungen und neue Arbeitgeber

17.10.1 Anforderungen an Einwilligungserklärungen

Die DSK hat sich aufgrund einer Eingabe mit der Frage befaßt, unter welchen Voraussetzungen Auskünfte durch die Dienstbehörde an private Dritte (insbesondere an Versicherungen) bei entsprechenden Anfragen erteilt werden dürfen. Folgende Fallgestaltung lag dem zugrunde: Im Rahmen der Inanspruchnahme einer privaten Berufsunfähigkeitsversicherung hat ein inzwischen im Ruhestand befindlicher Polizeibeamter gegenüber der Versicherung auf dem maßgeblichen Antragsformular folgende Klausel unterschrieben:

„Ich ermächtige die Versicherung, weitere ihr erforderlich erscheinende Auskünfte (z. B. von Ärzten, Krankenhäusern, Behörden, Sozialversicherungsträgern, anderen Versicherungsunternehmen) unmittelbar einzuholen und entbinde die befragten Personen bzw. Stellen hiermit ausdrücklich von der Schweigepflicht. Insbesondere erkläre ich mich damit einverstanden, daß Sozialversicherungsträger der Versicherung unter Befreiung von den Beschränkungen der §§ 35 SGB I, 67 f SGB X meine ärztlichen Unterlagen zur Verwendung im Verfahren zur Feststellung der Leistungen aus meiner Berufsunfähigkeitszusatzversicherung offenbaren."

Auf eine entsprechende Anfrage der Versicherung hin hat die Dienstbehörde aufgrund dieser Schweigepflichtentbindungsklausel die Vorgänge aus den Personalakten in Kopie übersandt, die das Verfahren auf Ruhestandsversetzung zum Gegenstand hatten. Aus der Sicht der DSK war zweifelhaft, ob eine derartige Einwilligungserklärung auf dem Formular zur Beantragung von Versicherungsleistungen tatsächlich die Dienstbehörde dazu ermächtigt, jede gewünschte Auskunft unmittelbar an die private Versicherung zu übermitteln. Sie hat der Dienstbehörde folgende Auffassung mitgeteilt:

„Zunächst ist schon fraglich, ob die allgemeine Formulierung in der Schweigepflichtentbindungsklausel, die von „Behörden" bzw. „Stellen" allgemein spricht, genügend bestimmt ist, um wirksam zu sein. Die DSK hat hier bereits erhebliche Zweifel. Den datenschutzgesetzlichen Anforderungen an eine Einwilligungserklärung (vgl. § 3 BDSG) entspricht sie jedenfalls nicht. Selbst wenn die Erklärung des Beamten auch unter diesem Gesichtspunkt zivilrechtlich wirksam sein sollte, hat die Behörde im Rahmen der verwaltungsrechtlichen Ermessensausübung jedenfalls zu berücksichtigen, ob die Einwilligungserklärung bestimmt und detailliert formuliert ist oder ob sie sehr allgemein und eher unbestimmt gestaltet ist. Im letzteren Fall sind im Zweifel Übermittlungen zu unterlassen. In Fällen der vorliegenden Art, in denen Leistungen Dritter an den Bediensteten in Rede stehen, wäre es dann angemessen, die fraglichen Informationen dem Bediensteten zuzuleiten, dem anheim zu stellen wäre, sie an seinen privaten Vertragspartner weiter zu übermitteln. Unmittelbare Datenübermittlungen sollten jedenfalls in Fällen derart weitgefaßter und unbestimmter Einwilligungserklärungen generell unterbleiben.

Im vorliegenden Fall dürfte die Versicherungsgesellschaft gegen die Regelung des § 2 Nr. 5 BB-BUZ (Besondere Versicherungsbedingungen für private Berufsunfähigkeitsversicherungen) verstoßen haben, als sie die in Rede stehende Information

erbeten hat (vgl. BGH, Urteil vom 14. Juni 1989, IV a ZR4/88, Versicherungsrecht 1989, S. 903). Da entsprechende rechtliche Beurteilungen für die übermittelnde Personaldienststelle grundsätzlich nicht möglich sein dürften, ist der von der DSK vorgeschlagene Weg wohl auch allein geeignet, die Dienststelle von Verwicklungen in privatrechtliche Auseinandersetzungen zwischen ihren Bediensteten und deren privaten Vertragspartnern freizuhalten."

Das Ministerium des Innern hat sich dieser Auffassung angeschlossen und seine nachgeordneten Behörden entsprechend informiert.

17.10.2 Grenzen für die Datenübermittlung zwischen altem und neuem Arbeitgeber

Aufgrund einer Eingabe hatte sich die DSK mit folgendem Sachverhalt zu befassen:

Der Beschwerdeführer war bei einer Kreisverwaltung als Angestellter tätig. Das Arbeitsverhältnis wurde durch einen Auflösungsvertrag beendet. Grund dafür waren Verfehlungen des Beschwerdeführers, die Gegenstand eines Ermittlungsverfahrens waren, das mit einem Strafbefehl abgeschlossen wurde.

Der Beschwerdeführer war daraufhin fünf Monate arbeitslos, bis er ein neues Arbeitsverhältnis mit einem privaten Arbeitgeber begründete. Am 2. Arbeitstag wurde dieses Arbeitsverhältnis aufgelöst, da der neue Arbeitgeber – von unbekannter Seite – über das vorangegangene Strafverfahren informiert worden war. Ein knappes Jahr darauf konnte der Beschwerdeführer eine neue Stelle im öffentlichen Dienst (bei einer Gemeinde eines anderen Bundeslandes) antreten. Diese Stelle verlor er nach acht Monaten. Grund dafür war, daß der Personalsachbearbeiter zu dieser Zeit telefonisch bei der Personalabteilung der Kreisverwaltung in Rheinland-Pfalz angefragt hat, welche Gründe seinerzeit zur Auflösung des Arbeitsvertrages mit dem Beschwerdeführer geführt hätten. Der Personalreferent hat seinen Kollegen in Hessen wahrheitsgemäß über den Strafbefehl informiert. Es war nicht aufzuklären, was der Anlaß dieser Anfrage war.

Die DSK hat den in Rede stehenden Übermittlungsvorgang zwischen dem Personalreferenten der rheinland-pfälzischen Kreisverwaltung und dem Personalsachbearbeiter der hessischen Gemeinde wie folgt beurteilt:

Personalvorgänge sind grundsätzlich vertraulich zu behandeln. Ein bisheriger Arbeitgeber ist zwar dann berechtigt, auch ohne Zustimmung des betroffenen Arbeitnehmers Auskünfte über dessen Person und Verhalten zu erteilen, wenn der Datenempfänger ein berechtigtes Interesse an der Auskunft geltend machen kann, und wenn schutzwürdige Belange des betroffenen Arbeitnehmers nicht entgegenstehen. Ein solches berechtigtes Interesse besteht grundsätzlich jedoch nur dann, wenn der anfragende Arbeitgeber beabsichtigt, den betroffenen Arbeitnehmer einzustellen. Die dann zulässige Auskunft muß wie ein Zeugnis wahr im Sinne einer vollständigen, gerechten und nach objektiven Grundsätzen durchgeführten Beurteilung sein. Eine das Zeugnis ergänzende Auskunft ist nur gegenüber dem nächstfolgenden Arbeitgeber zulässig (so auch Schaub, Arbeitsrechtshandbuch, § 147.2; Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, S. 112, Tz. 1.3.2.2).

Im vorliegenden Fall war nicht dem nächstfolgenden Arbeitgeber, sondern im zeitlichen Abstand von über zwei Jahren einem anderen Arbeitgeber gegenüber eine Auskunft über persönliche Umstände eines ehemaligen Arbeitnehmers erteilt worden, die grundsätzlich vertraulich zu behandeln sind.

Mit der entsprechenden Informationsübermittlung war zudem eine Änderung des Zwecks der Information verbunden, der von der zuständigen Staatsanwaltschaft mit der Zusendung des Strafbefehls an die Kreisverwaltung beabsichtigt war. Diese Datenübermittlung beruhte auf Nr. 15 der „Anordnung über Mitteilungen in Strafsachen". Sie war an den Leiter der Behörde zu adressieren und als „vertrauliche Personalsache" zu kennzeichnen. Ihr Zweck ist es, dem öffentlichen Arbeitgeber zu ermöglichen, die Durchführung von Maßnahmen zu prüfen, die unter dem Gesichtspunkt der besonderen Situation des öffentlichen Dienstes gegenüber einem Bediensteten erforderlich erscheinen, der straffällig geworden ist. Sobald diese Prüfung durch den Arbeitgeber abgeschlossen ist, ist der Zweck der Mitteilung erfüllt. Dieser Zweck besteht keinesfalls darin, dem Arbeitgeber eine „Warnfunktion" gegenüber späteren Arbeitgebern zu ermöglichen.

Die DSK hat in der hier erfolgten Datenübermittlung einen Verstoß gegen datenschutzrechtliche Vorschriften gesehen. Sie hat die betroffene Kreisverwaltung darauf hingewiesen und zur künftigen Beachtung der genannten Grundsätze aufgefordert.

17.11 Ehrensold-Versicherung für kommunale Ehrenbeamte

Über das Ministerium des Innern und für Sport hat der LfD erfahren, daß der Gemeinde- und Städtebund seinen Verbandsmitgliedern empfohlen hat, Ehrensoldversicherungen mit der „Bayern-Versicherung" abzuschließen, wobei sich die Bedingungen dieser Ehrensoldversicherung an einem Empfehlungsvertrag zwischen dem Gemeinde- und Städtebund einerseits, der Bayern-Versicherung andererseits orientieren sollen.

Aus folgendem Grund haben sich datenschutzrechtliche Bedenken ergeben: Die private Versicherung verlangt zur Risikoeinschätzung Informationen, die unter anderem auch den Gesundheitszustand der betroffenen Ehrenbeamten zum Gegenstand haben. Zur Durchführung des öffentlich-rechtlichen Amtsverhältnisses dieser Amtsträger wäre eine Erhebung dieser Daten nicht erforderlich.

Die Gemeinden befinden über den Abschluß der Ehrensoldversicherungen, ohne daß die betroffenen Amtsträger darauf einen entscheidenden Einfluß hätten; nach Abschluß einer solchen Versicherung dürfte für diese wohl kaum eine praktische Möglichkeit bestehen, ihre Mitwirkung an der Durchführung des Ehrensoldversicherungsvertrages (etwa durch Weigerung der Beantwortung der gesundheitlichen Fragen) zu versagen. Zumindest besteht ein starker faktischer Druck, sich diesen Anforderungen zu unterwerfen, um nicht im politischen Raum dem Vorwurf ausgesetzt zu sein, die Gemeinde finanziell zu belasten.

Aus der Sicht des Datenschutzes ist zur datenschutzgerechten Ausgestaltung des Verfahrens folgendes erforderlich:

a) Wenn eine Ehrensoldversicherung in der geplanten Form für erforderlich gehalten wird, sind die betroffenen Amtsträger ausdrücklich darauf hinzuweisen, daß es ihnen freisteht, an der Durchführung dieses Vertrages durch die Preisgabe gesundheitlicher Daten mitzuwirken oder nicht. Bei einer Verweigerung der Einwilligung dürfen den Amtsträgern keine Nachteile entstehen. Auch darauf sind sie hinzuweisen.

b) Falls die Einwilligung der Amtsträger erteilt wird, sollte gewährleistet werden, daß die Datenerhebung unmittelbar durch die Versicherung erfolgt; eine Funktion der betroffenen Gemeinde als „Briefträger" in diesem Zusammenhang, die dazu führen würde, daß auch die Gemeinde detaillierte Informationen über den Gesundheitszustand ihrer Amtsträger erhält, sollte vermieden werden.

c) Wenn die Höhe der Prämienzahlung vom Gesundheitszustand der Bediensteten abhängig ist, wird aus einem Vergleich der Prämien deutlich, welches Risiko der Berufsunfähigkeit durch die Versicherung zugrunde gelegt wird. Nicht nur unter dem Aspekt, daß der Haushalt der Gemeinde grundsätzlich öffentlich beraten wird, könnte auch in diesem Zusammenhang ein datenschutzrechtlicher Gefährdungspunkt bestehen. Die betroffenen Amtsträger sind deshalb hierüber deutlich zu informieren, bevor ihre Einwilligung erbeten wird.

Diese Gesichtspunkte folgen aus dem Grundrecht auf informationelle Selbstbestimmung, das auch die Ehrenbeamten schützt. Eingriffe in dieses Recht sind nur aufgrund eines Gesetzes zulässig. Weder das Ehrensoldgesetz noch andere Gesetze sehen entsprechende Eingriffsbefugnisse vor. Außerdem ist anzumerken, daß die Wahrnehmung von Ehrenämtern nicht über das gesetzlich gebotene Maß hinaus erschwert werden sollte. Das Ministerium des Innern hat die Bedenken des LfD in einem Schreiben an den Gemeinde- und Städtebund geteilt. Der Gemeinde- und Städtebund hat alle genannten datenschutzrechtlichen Anforderungen akzeptiert und seine Rundschreiben entsprechend ergänzt.

17.12 Führung von Personalnebenakten

Die Personalabteilung einer Universität hat die Vorlage eines Anstellungsvertrages eines wissenschaftlichen Mitarbeiters an den zuständigen Hochschullehrer unter Hinweis auf den Datenschutz verweigert. Als Argument wurde angeführt, die Führung „doppelter Personalakten" sei unzulässig.

Eine Überprüfung aus datenschutzrechtlicher Sicht hat folgendes ergeben:

Die Aufbewahrung eines Anstellungsvertrages mit einem wissenschaftlichen Mitarbeiter beim unmittelbaren Dienstvorgesetzten dürfte als Führung einer Personalnebenakte im Sinne der Nr. 2.6 der Verwaltungsvorschrift der Landesregierung zur Führung der Personalakten vom 23. Dezember 1985 anzusehen sein. Danach können „bei Bedarf" Personalnebenakten geführt werden. In die Personalnebenakten dürfen nur solche Vorgänge aufgenommen werden, die auch in den Personalhauptakten oder Personalbeiakten enthalten sind.

Es unterliegt wohl keinem Zweifel, daß es für den unmittelbaren Dienstvorgesetzten (insbesondere auch unter Berücksichtigung der besonderen Bedingungen, unter denen wissenschaftliche Mitarbeiter für Hochschullehrer tätig sind) erforderlich ist, genau zu wissen, welche rechtlich bindenden Vereinbarungen mit einem nachgeordneten Bediensteten getroffen worden sind, vor allem, welche Verpflichtungen dieser gegenüber der Anstellungsbehörde eingegangen ist. Auf deren Einhaltung hat der unmittelbare Dienstvorgesetzte zu achten. Damit dürfte nicht nur ein Bedarf für die Führung einer solchen Personalnebenakte bestehen, es dürfte sich um ein Erfordernis zur Durchführung des Arbeitsverhältnisses handeln.

17.13 Adoptionsunterlagen in Besoldungsakten

Adoptiveltern sind erfahrungsgemäß in Datenschutzangelegenheiten besonders sensibilisiert. Sie wissen, welch fatale Folgen es

haben kann, wenn etwa die frühere Identität eines adoptierten Kindes durch Unachtsamkeit aufgedeckt wird, und fordern deshalb immer wieder, daß die durch das Adoptionsgeheimnis (§ 1758 BGB) besonders geschützten Informationen unter besonders strenger Beachtung des Erforderlichkeitsprinzips nur dann gespeichert oder zu den Akten genommen werden, wenn dies zur Aufgabenerfüllung zwingend erforderlich ist.

Ein öffentlich Bediensteter, der seine personalaktenführende Stelle um Löschung der Adoptionsdaten in den Besoldungsakten gebeten hatte, erhielt den Bescheid, daß seinem Ersuchen nicht entsprochen werden könne, denn die in den Akten befindlichen Unterlagen – Geburtsurkunden, Adoptionsbeschluß – seien zur Festsetzung von Ortszuschlag und Kindergeld erforderlich. Die Geburtsurkunde diene als Nachweis für die Existenz eines Kindes sowie des Geburtsdatums. Dieses sei erheblich für die Dauer der Kindergeldzahlung; gem. § 2 Abs. 2 BKGG könne Kindergeld, von den gesetzlich normierten Ausnahmefällen abgesehen, regelmäßig nur bis zur Vollendung des 16. Lebensjahres gewährt werden. Der Adoptionsbeschluß sei insoweit von Bedeutung, als von dem in diesem Beschluß genannten Zeitpunkt an eine Gleichstellung mit leiblichen Kindern erfolge. Da Ortszuschlag und Kindergeld laufend gewährt würden, seien die genannten Unterlagen – auch nach der Festsetzung – als ständige Nachweise für das Vorliegen der Zahlungsvoraussetzungen notwendig. Ferner dienten sie der Dokumentation einer ordnungsmäßigen Zahlung in der Vergangenheit. Die gesamten Auszahlungsvorgänge unterlägen der Prüfungsbefugnis des Rechnungshofs und dies erfordere die Vollständigkeit der Akten. Außerdem bestehe schon deshalb kein datenschutzrechtliches Problem, weil die fraglichen Daten für die Erbringung einer Sozialleistung – Kindergeld – erhoben und verarbeitet würden und deshalb durch das Sozialgeheimnis geschützt seien. Sie dürften nur beim Vorliegen der Voraussetzungen der §§ 68 bis 77 SGB X übermittelt werden.

Gerade dieses letzte Argument verdeutlicht indessen, daß die Rechtslage von der aktenführenden Stelle falsch beurteilt wurde. Es blieb nämlich unberücksichtigt, daß § 1758 Abs. 1 BGB eine ergänzende Offenbarungsvoraussetzung nennt, die stets zu berücksichtigen ist, nämlich das Vorliegen besonderer Gründe des öffentlichen Interesses. Für eine Offenbarung von Adoptionsdaten genügt also nicht das Vorliegen der Voraussetzungen nach dem SGB X, also beispielsweise die Erforderlichkeit zur Aufgabenerfüllung (§ 69 Abs. 1), sondern es muß – im Sinne eines Zweischrankenprinzips – geprüft werden, ob auch die Voraussetzungen des § 1758 Abs. 1 BGB vorliegen.

Im übrigen – so die DSK – ließe sich das Problem des Nachweises der Anspruchsvoraussetzungen unter Wahrung des Adoptionsgeheimnisses in der Weise lösen, daß die bei den Akten befindliche Geburtsurkunde mit dem früheren Namen des Kindes sowie der Adoptionsbeschluß durch eine Geburtsurkunde nach § 62 Abs. 2 Personenstandsgesetz ersetzt wird.

Der Rechnungshof Rheinland-Pfalz nahm zu der von der aktenführenden Stelle behaupteten Notwendigkeit Stellung, die Adoption in den Akten für Prüfungszwecke nachzuweisen. Er stimmte mit der DSK in der Auffassung überein, daß es für Prüfungszwecke nicht erforderlich ist, die frühere Identität adoptierter Kinder in den Besoldungsakten zu erfassen. Es genüge, wenn der Festsetzungsbehörde neben der Geburtsurkunde des adoptierten Kindes nach § 62 Abs. 2 Personenstandsgesetz der Adoptionsbeschluß des Vormundschaftsgerichts lediglich zur Einsichtnahme vorgelegt werde und die Festsetzungsbehörde den Zeitpunkt des Wirksamwerdens des Adoptionsbeschlusses durch Aktenvermerk festhalte. In einem zu den Akten genommenen Adoptionsbeschluß seien die früheren Namen der Kinder zu löschen (zu schwärzen).

Der Vorgang konnte abgeschlossen werden, nachdem die aktenführende Stelle die Rechtsauffassung der DSK und des Rechnungshofs Rheinland-Pfalz anerkannte.

17.14 Datenerhebungen und -speicherungen bei einem Verdacht auf Dienstvergehen sowie im Verfahren zur Zwangspensionierung

17.14.1 Schranken der Datenerhebung und -speicherung bei Ermittlungen des Dienstvorgesetzten wegen des Verdachts eines Dienstvergehens

In einer Eingabe an den Bürgerbeauftragten hatte ein Beamter ausgeführt:

„Es ist daher in keiner Weise nachvollziehbar, wie es bei der geschilderten Sachlage zu einer derartigen Verzögerung bei der Beförderung gekommen ist. Mir sind durch diese Verzögerungen hohe Verluste entstanden, so daß Konkursgefahr droht. Da es sich um die Frage der finanziellen Existenz handelt, darf ich nochmals bitten, für eine gerechte Entscheidung zu sorgen."

Der Mittelbehörde wurde diese Eingabe durch den Bürgerbeauftragten mit der Bitte um Stellungnahme vorgelegt. Diese hat dem unmittelbaren Dienstvorgesetzten Kopien der Schreiben des Beamten an den Bürgerbeauftragten mit der Bitte um Kenntnisnahme übersandt. Im Hinblick auf die von dem Beamten behauptete „drohende Konkursgefahr" hat sie gebeten, diesen „zu einer ausführlichen Erklärung über seine vermögensrechtliche Situation zu veranlassen."

Daraufhin wurde der Beamte durch den Vorgesetzten über seine private Vermögenssituation befragt. Darüber wurde ein Protokoll gefertigt und der Mittelbehörde vorgelegt.

Mit Verfügung der Mittelbehörde wurde die Durchführung von Vorermittlungen gem. § 26 Abs. 2 DOG angeordnet. Gegenstand dieser Vorermittlungen sollte neben der Frage der Konkursgefahr die dienstordnungsrechtliche Würdigung der Angabe des betroffenen Beamten sein, die Nichtbeförderung sei eine Willkürentscheidung gewesen.

Daraufhin wurden Vorermittlungen angeordnet und der Beamte gleichzeitig gem. § 26 Abs. 2 DOG belehrt. Zwei Monate später wurde das Verfahren eingestellt.

Die Niederschrift über die Befragung wird nach wie vor in den Personalakten des Beamten aufbewahrt.

Mit seiner Eingabe hat der betroffene Beamte die DSK um Stellungnahme dazu gebeten, ob es zulässig sei, seine persönlichen Daten im Wege einer Befragung, so wie diese erfolgt sei, zu erheben und eine entsprechende Niederschrift zu den Personalakten zu nehmen. Er hat ausdrücklich gleichzeitig der DSK schriftlich Vollmacht zur Einsichtnahme in sämtliche Akten erteilt.

Der Dienstvorgesetzte hat das Anfrageschreiben der DSK zum Anlaß genommen, den betroffenen Beamten darüber zu befragen, ob es zutreffend sei, daß er der DSK Vollmacht zur Akteneinsicht erteilt habe. Außerdem hat er ihn dazu befragt, ob es zutreffend sei, daß er gegenüber der DSK gerügt habe, er sei vorher über den Gegenstand des Gesprächs im Dezember 1989 nicht unterrichtet worden. Auch über das Ergebnis dieser Befragung wurde eine Protokollnotiz gefertigt, die ebenfalls zu den Personalakten genommen worden sein dürfte.

Der Beamte hatte zwischenzeitlich den LfD schriftlich darum gebeten, zu veranlassen, daß er in dieser Angelegenheit nicht mehr zum Vorgesetzten beordert werde. Er bat um Unterstützung und Hilfe, da er sich in seinen Entscheidungen nicht mehr frei fühle, wenn er zum Dienstvorgesetzten gerufen werde. Unter datenschutzrechtlichen Gesichtspunkten wurde die Angelegenheit wie folgt gewürdigt:

a) Die Befragung vor Einleitung des Vorermittlungsverfahrens könnte als allgemeine Überwachungsmaßnahme des Dienstvorgesetzten zulässig sein. Aus datenschutzrechtlicher Sicht bestehen gewisse Bedenken gegen diese Würdigung, da angesichts des konkreten Anlasses der Befragung, die die Vermögenssituation des Beschwerdeführers zum Gegenstand hatte, wegen der Nähe entsprechender Vorgänge zu dienstordnungsrechtlich relevanten Tatbeständen (leichtfertiges Schuldenmachen) eine Vernehmung des Beamten außerhalb der dem Schutz des Betroffenen dienenden Voraussetzungen des Vorermittlungsverfahrens des DOG wohl kaum als zulässig angesehen werden kann (vgl. Lindgen, Handbuch des Disziplinarrechts, 2. Band, Berlin 1968, S. 423 f). In diesem Zusammenhang ist auch nicht ohne Bedeutung, daß außerdienstliche Verhältnisse thematisiert worden sind und daß ein Protokoll gefertigt werden sollte.

b) Unabhängig von der Frage, ob diese Befragung formlos zulässig gewesen ist, oder ob sie im Rahmen der Vorgaben des § 26 Abs. 2 DOG als Maßnahme disziplinarrechtlicher Vorermittlungen hätte durchgeführt werden müssen, steht fest, daß sämtliche Schriftstücke, die sich auf die „drohende Konkursgefahr" des Beamten beziehen und außerhalb des Vorermittlungsverfahrens entstanden sind, aus der Personalakte des Beamten zu entfernen sind, soweit sie nicht Teil des Vorermittlungsverfahrens geworden sind. Dies ergibt sich aus Nr. 4.1 der Verwaltungsvorschrift der Landesregierung über die Führung der Personalakten. Danach sind Vorgänge über Tatsachen, die sich als unrichtig erweisen, aus den Personalakten zu entfernen und zu vernichten, falls nicht der Beamte widerspricht. Dies gilt auch für alle Vorgänge, die auf diese Tatsachenbehauptungen oder Werturteile hinweisen.

c) Es war darauf hinzuweisen, daß die im Zusammenhang mit dem Vorermittlungsverfahren nach § 26 Abs. 1 DOG entstandenen Vorgänge zwei Jahre nach Einstellung des Vorermittlungsverfahrens zu vernichten sind (§ 108 Abs. 1 i. V. m. Abs. 6 DOG).

d) Die Befragung des Beamten anläßlich der Anfrage der DSK stößt auf gewisse Bedenken:

Die DSK hatte in ihrem Anfrageschreiben ausdrücklich ausgeführt, sie sei vom Beschwerdeführer zur Einsichtnahme in die Personalakten bevollmächtigt. Unabhängig davon, daß dies nach der gesetzlichen Lage (§ 20 LDatG) keine Voraussetzung der Auskunftspflicht befragter öffentlicher Stellen ist, bestand kein Anlaß, die Angaben der DSK durch eine Befragung des Betroffenen zu überprüfen. Dies gilt auch für den Passus des Schreibens der DSK, der Beschwerdeführer sei vorher über den Gegenstand des Gesprächs nicht unterrichtet worden. Damit war gemeint, daß vor dem Gespräch keine Ladungs- oder Einlassungsfrist gewährt worden ist. Dieser Sinn des Schreibens der DSK hätte durch eine Rückfrage bei ihr geklärt werden können; ein Anlaß, den Beamten dazu zu hören, bestand nicht.

Der LfD hat Verständnis dafür, daß der Beamte sich durch eine derartige Befragung beeinträchtigt fühlt. Es ist generell unangemessen und mit dem Sinn des Anrufungsrechts des LDatG nur schwer vereinbar, daß eine Eingabe bei der DSK bzw. beim LfD zum Anlaß von dienstlichen Maßnahmen genommen wird, die von dem Betroffenen verständlicherweise als beeinträchtigend und belastend empfunden werden.

e) Eine Aufnahme der Vorgänge, die sich auf die Eingabe des Betroffenen an die DSK bzw. an den LfD beziehen, in die Personalakte trifft ebenfalls unter dem Gesichtspunkt auf Bedenken, daß damit die Ausübung des Anrufungsrechts des § 15 LDatG Folgen nach sich zieht, die vom Betroffenen als nachteilig angesehen werden können und daß demzufolge möglicherweise öffentlich Bedienstete von einer Wahrnehmung dieses Rechts abgehalten werden. Unabhängig davon gilt im vorliegenden Fall zumindest die Regelung des § 108 Abs. 6 DOG: Die Eingabe bezog sich auch auf Vorgänge im Zusammenhang mit dem durchgeführten disziplinarrechtlichen Vorverfahren. Alle diesbezüglichen Schriftstücke wären demnach spätestens nach Ablauf der o. g. Frist aus der Personalakte zu entfernen und zu vernichten.

17.14.2 Datenerhebungen im Zwangspensionierungsverfahren

Ein Lehrer, der längere Zeit wegen psychischer Störungen krank gewesen war, sollte nach Auffassung der zuständigen Bezirksregierung zwangsweise in den Ruhestand versetzt werden. Zu diesem Zweck wurde gegen ihn ein Ermittlungsverfahren gem. § 58 LBG durchgeführt. Der Lehrer wurde aufgefordert, sich einer psychologischen Begutachtung zur Verfügung zu stellen. Zur Vorbereitung dieser Begutachtung wurden seine vollständigen Personalakten an einen Psychologen übersandt, der eine schriftliche Auswertung fertigte. Fraglich war,

- ob eine Pflicht bestand, sich einer psychologischen Begutachtung zu unterziehen,

- ob die Aktenübersendung zulässig war sowie

- ob ggf. ein Anspruch des Beschwerdeführers auf Entfernung dieser psychologischen Bewertung seiner Persönlichkeit aus den Personalakten bestand.

Aus datenschutzrechtlicher Sicht hat die DSK Bedenken gegen die Beiziehung eines Psychologen im Ermittlungsverfahren gem. § 58 LBG geäußert. § 56 Abs. 1 letzter Satz LBG enthält die Vorschrift, wonach der Beamte bei Zweifeln über die Dienstunfähigkeit verpflichtet ist, sich nach Weisung der Behörde ärztlich untersuchen und, falls ein Amtsarzt dies für erforderlich hält, beobachten zu lassen. Die Beschränkung der Pflicht des Beamten darauf, sich einer ärztlichen Untersuchung zu unterziehen, gilt grundsätzlich auch für das Ermittlungsverfahren nach § 58 LBG. Der Gutachter muß als Arzt eine besondere Qualifikation besitzen, krankhafte, auf Dauer angelegte Faktoren, die zur Dienstunfähigkeit führen, festzustellen. Auch eine andere Überlegung führt zum Ergebnis, daß die Beauftragung eines Psychologen in Ermittlungsverfahren der vorliegenden Art unzulässig ist: Dienstunfähigkeit liegt nach dem LBG dann vor, wenn ein körperliches Gebrechen oder Schwäche der körperlichen oder geistigen Kräfte zur Nichterfüllbarkeit von Dienstpflichten führen. Die Schwäche geistiger Kräfte im Sinne des Gesetzes ist zwar auch dann gegeben, wenn der Beamte im Schuldienst geistigen Erschütterungen nicht mehr gewachsen ist oder infolge der Erkrankung eine Abwehrstellung der Schüler und damit eine Störung des Lehrbetriebes zu erwarten ist. Es ist jedoch davon auszugehen, daß Bestandteil der gesetzlichen Definition eine Schwäche im Sinne einer auf Dauer angelegten krankhaften Persönlichkeitsbeeinträchtigung ist. Für die Diagnose von Krankheiten auch im weiteren Sinn ist aber nicht der Psychologe – so hilfreich seine Erkenntnisse bei der therapeutischen Betreuung psychischer Erkrankungen auch sein mögen – sondern der Arzt, und hier der psychiatrische Facharzt, berufen. Voraussetzung der Zwangspensionierung ist eine ärztlich diagnostizierbare Beeinträchtigung. Die Feststellung einer bloß psychologisch erkennbaren Beeinträchtigung, die den Bediensteten an einer umfassenden Ausnutzung seiner körperlichen und geistigen Möglichkeiten hindert oder die seine Empfindungs- und Glücksfähigkeit verringert, ist insofern grundsätzlich nicht erforderlich. Dies wurde im vorliegenden Fall insbesondere auch durch die Formulierungen des eingeschalteten Psychologen deutlich, der eine psychologische Beurteilung des Beschwerdeführers unter folgenden Aspekten für erforderlich angesehen hat: Es sollte eine Würdigung der Gesamtpersönlichkeit des Beschwerdeführers unter Zuhilfenahme der Persönlichkeitspsychologie, der Neurosepsychologie, von pädagogisch-berufspsychologischen Erkenntnissen, der Partnerschaftspsychologie sowie der Sozialpsychologie erfolgen. Die mit einer solchen psychologischen Gesamtschau zwangsläufig verbundenen Wertungen und Eingriffe in den Kernbereich der Persönlichkeit des Betroffenen dürften sich gerade nicht auf den entscheidungsrelevanten Teil der Beurteilung der Leistungsfähigkeit im Sinne der Dienstfähigkeit des Lehrers beschränken, sie dürften vielmehr die Gesamtpersönlichkeit in all ihren Aspekten umfassen. Damit ist eine entsprechende Begutachtung – wenn überhaupt – nur in seltenen Ausnahmefällen zulässig.

Ein solcher Ausnahmefall lag im von der DSK zu beurteilenden Fall jedenfalls nicht vor.

Dementsprechend hat sie auch die Übersendung der Personalakten an den Psychologen zum Zweck einer psychologischen Aktenauswertung für unzulässig gehalten; sie hat die Entfernung der schriftlichen Begutachtung aus den Personalakten gefordert.

Die Angelegenheit, die zwischenzeitlich gerichtshängig geworden war, wurde durch einen Vergleich auf Vorschlag des Gerichts beendet, wonach sich das beklagte Land verpflichtet hat, die beanstandete gutachterliche Äußerung des Psychologen aus den Personalakten insgesamt zu entfernen und zu vernichten. Auf die Durchführung einer persönlichen psychologischen Begutachtung wurde verzichtet.

17.15 Frauenförderungsgesetz
Welche datenschutzrechtlichen Grenzen gelten für die Arbeit von Frauenbeauftragten?

Anläßlich der Einbringung eines Gesetzentwurfs zur Frauenförderung durch die Fraktionen der CDU und der F.D.P. hat sich die DSK mit datenschutzrechtlichen Fragen in diesem Zusammenhang befaßt. Die Frage, welche Informationsrechte Frauenbeauftragte besitzen sollen und welche verfassungsrechtlichen Schranken hierfür bestehen, dürfte für die Regierung grundsätzlich bedeutsam sein.

Die DSK ging davon aus, daß das Ziel einer umfassenden Kompetenzausstattung der Frauenbeauftragten mit dem informationellen Selbstbestimmungsrecht der Bediensteten und der Bewerber kollidieren kann. Sie war sich allerdings auch bewußt, daß jede wertende Betrachtung der Verhältnismäßigkeit von Eingriffen in das informationelle Selbstbestimmungsrecht in diesem Zusammenhang dem Vorwurf ausgesetzt ist, das politische Ziel der Frauenförderung nicht im gebotenen Umfang anzuerkennen. Sie hat deshalb den eindeutigen politischen Willen, von dem die Einrichtung von Frauenbeauftragten getragen ist, vor dem Hintergrund eines weiten Gestaltungsspielraums des Gesetzgebers besonders berücksichtigt. Dennoch hielt sie folgende kritische Anmerkungen für geboten:

a) Nach den seinerzeitigen Überlegungen sollte die Frauenbeauftragte bei allen Personalauswahlgesprächen beteiligt werden. Dies bedeutet datenschutzrechtlich, daß während der Phase der Datenerhebung eine zusätzliche Stelle Kenntnis von den Daten erhält, die der Bewerber preisgibt. Da diese Verfahrensweise ohne Einwilligung der Betroffenen möglich sein soll, ist sie als Eingriff in deren informationelles Selbstbestimmungsrecht zu werten. Zulässig sind solche Eingriffe dann, wenn sie im überwiegenden Allgemeininteresse geboten sind. Die DSK hat sich dafür ausgesprochen, unter dem Gesichtspunkt der Verhältnismäßigkeit des Eingriffs ein solches Anwesenheitsrecht nur für die Fälle vorzusehen, in denen eine Konkurrenzsituation zwischen männlichen und weiblichen Bewerbern besteht. Falls also in einem Bewerbungsverfahren nur männliche oder nur weibliche Bewerber in Betracht kommen, sollte dieses Anwesenheitsrecht entfallen. Dementsprechend sollte eine gesetzliche Formulierung gewählt werden, die dieses Anwesenheitsrecht an die Erforderlichkeit zur Aufgabenerfüllung der Frauenbeauftragten knüpft.

b) Auch die Frage des Umfangs des Informationsrechts der Frauenbeauftragten ist datenschutzrechtlich bedeutsam. Vorgesehen war, daß zwar die Einsicht in Personalakten an die Einwilligung der Betroffenen geknüpft sein sollte. Alle sonstigen Informationsübermittlungen sollten jedoch ohne weitere Schranke erfolgen. Auch hier hat die DSK, soweit personenbezogene Daten betroffen sind, eine strikte Anknüpfung an den Erforderlichkeitsgrundsatz für geboten gehalten.

c) Eine besondere Verpflichtung zur Verschwiegenheit, wie sie etwa für Personalräte besteht, ist auch für die Frauenbeauftragten zu schaffen. Nur damit würde klargestellt werden, daß ihre gesetzlichen Aufgaben nicht zu unbegrenzten Datenübermittlungen an andere Stellen berechtigen.

d) Schließlich sollte geklärt werden, daß vorgesehene Datenübermittlungen an übergreifend zuständige Frauenbeauftragte (Frauenbeauftrage des Geschäftsbereichs der obersten Dienstbehörde sowie Leitstelle für Frauenfragen) nur in begründeten Einzelfällen mit Zustimmung der Betroffenen erfolgen dürfen, daß bei diesen zentralen Stellen also keine umfassenden personenbezogenen Datenbestände geschaffen werden dürfen.

Wegen verfassungsrechtlicher Bedenken bezüglich der Quotenregelung wurde das weitere Gesetzgebungsverfahren unterbrochen. Sollte ein neues Gesetzgebungsvorhaben zu diesem Gegenstand eingeleitet werden, sind die genannten Gesichtspunkte zu berücksichtigen.

18 Medien

18.1 ZDF-Staatsvertrag

Die Regelungen über den Datenschutz beim ZDF finden sich zur Zeit noch im Landesdatenschutzgesetz (§ 24 „Sonderbestimmungen für die Gerichte und das Zweite Deutsche Fernsehen"), da Rheinland-Pfalz das Sitzland der Länderanstalt ist.

Die im Staatsvertrag über das Zweite Deutsche Fernsehen getroffenen Regelungen über den Datenschutz hindern, wenn sie voraussichtlich am 1. Januar 1992 geltendes Recht geworden sind, den Landesgesetzgeber daran, den Datenschutz beim ZDF wie bisher selbst zu regeln. Hierfür hätte sich die in kürzester Frist anstehende Novellierung des Landesdatenschutzgesetzes angeboten. Der Vorschlag des LfD, diese Möglichkeit offenzuhalten, war aber bei den Verhandlungen über den Staatsvertrag nicht durchsetzbar. Der Landesregierung, die sich insbesondere für die vom LfD vorgebrachten Anliegen eingesetzt hat, ist hierfür auch an dieser Stelle ausdrücklich zu danken.

Der LfD hatte in einem Schreiben an die Staatskanzlei eine Reihe klärungsbedürftiger Fragen angesprochen:

So wird die Auskunft an einen Betroffenen über die der Berichterstattung zugrundeliegenden zu seiner Person gespeicherten Daten davon abhängig gemacht, daß er durch die Berichterstattung in seinem Persönlichkeitsrecht bereits beeinträchtigt ist. Das ZDF kann durch Negieren dieser Voraussetzung bis hin zur gerichtlichen Entscheidung die Geltendmachung des Anspruchs blockieren. Die weiteren in drei Punkten in § 17 Abs. 3 aufgezählten Verweigerungsgründe, die insgesamt das sog. Redaktionsgeheimnis zum Gegenstand haben, erscheinen zunächst als Systembruch, da sie im Grunde nur bei einem uneingeschränkten Auskunftsanspruch plausibel sind. So wirken sie bei bereits vorliegender Rechtsverletzung als zusätzliche Einschränkung.

Das Auskunftsrecht ist immerhin der Kern des Rechts auf informationelle Selbstbestimmung, denn ohne Kenntnis der zu seiner Person gespeicherten Daten kann kein Betroffener seine weiteren Rechte, nämlich die Berichtigung oder das Hinzufügen einer eigenen Darstellung, wirksam wahrnehmen. Die dem Betroffenen gegebenen Rechte werden durch die gesamte Regelung praktisch wirkungslos gemacht. Die Folge ist eine nicht hinnehmbare Aushöhlung des hier in Frage stehenden Grundrechts.

Begrüßt wird, daß aufgrund der Neuregelung in § 18 Abs. 8 sich jedermann unmittelbar an den Beauftragten des ZDF für den Datenschutz wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch das ZDF in seinen schutzwürdigen Belangen verletzt zu sein.

Gleiches gilt auch für die Ausgestaltung seiner Rechte gegenüber der Anstalt auf Auskunft, Akteneinsicht und Zutritt zu allen Diensträumen (§ 18 Abs. 3 Ziff. 1 und 2), wenn diese Rechte nur im Rahmen einer anstaltsinternen Datenschutzkontrolle bestehen.

Von der Möglichkeit, die Kontrolle des Datenschutzes hinsichtlich der nicht dem journalistisch-redaktionellen Bereich unterliegenden Verwaltungsdaten (z. B. Personaldaten der Bediensteten) einer anstaltsexternen unabhängigen Instanz zu übertragen, wurde kein Gebrauch gemacht. Immerhin hat das Bundesverfassungsgericht in seinem Volkszählungsurteil eine unabhängige Datenschutzkontrolle gefordert.

Schließlich ist aber zu begrüßen, daß in § 18 Abs. 7 die im LDatG enthaltene Regelung übernommen wurde, daß der Datenschutzbeauftragte des ZDF seinen im Zeitabstand von zwei Jahren zu erstattenden Bericht auch dem Landesbeauftragten für den Datenschutz zusendet. Diese Regelung hat sich in der Vergangenheit bewährt und zu einer Reihe fruchtbarer Gespräche zwischen dem ZDF-Beauftragten und der DSK geführt. Bei Fortführung dieser positiven Praxis wird sich auch in Zukunft die eine oder andere Frage im Sinne eines für den Bürger bestmöglichen Datenschutz klären lassen.

18.2 Rundfunkstaatsvertrag

Wie bereits in der Präambel festgehalten, enthält der Rundfunkstaatsvertrag unter Berücksichtigung der europäischen Entwicklung grundlegende Regelungen sowohl für den öffentlich-rechtlichen wie für den privatrechtlich organisierten Rundfunk in dem dualen Rundfunksystem der Länder des vereinten Deutschlands.

Die in § 28 enthaltene Bestimmung über den Datenschutz enthält alle notwendigen Festlegungen für eine datenschutzgerechte Verarbeitung der in diesem Zusammenhang anfallenden Informationen. Die Verhandlungen über die nähere Gestaltung wurden für die Datenschutzbeauftragten abredegemäß vom Berliner Datenschutzbeauftragten geführt. Für die Rundfunkreferenten der Länder handelte die Niedersächsische Staatskanzlei.

Für den LfD Rheinland-Pfalz ging es dabei um die Fortgeltung der Kontrollregelungen des § 34 Abs. 2 bis 4 des Landesrundfunkgesetzes. Da § 28 Abs. 1 mit der Formulierung „soweit nichts anderes bestimmt ist", das entsprechende Landesrecht unberührt läßt, ist davon auszugehen, daß die Kontrollbestimmungen des § 34 Abs. 2 bis 4 des Landesrundfunkgesetzes ohne Beeinträchtigung fortbestehen, da es sich bei ihnen ausschließlich um Verfahrensregelungen handelt und der Staatsvertrag für den Datenschutz insoweit nur materielles Datenschutzrecht setzt. Auf schriftliche Anfrage des LfD hat die Staatskanzlei mit Schreiben vom 31. Mai 1991 diese Rechtsauffassung im Ergebnis ausdrücklich bestätigt. Der öffentlich-rechtliche Bereich wird durch die im Staatsvertrag vorgesehene Regelung ohnehin nicht tangiert; er bleibt den Regelungen der einzelnen Länder über ihre Landesrundfunkanstalten vorbehalten.

18.3 Rundfunkgebührenstaatsvertrag

Die DSK hat in den verschiedenen Entwurfsphasen durch detaillierte Stellungnahmen gegenüber der Landesregierung und den Datenschutzbeauftragten anderer Länder ihre Vorstellungen erhoben. Schwerpunkte waren der Katalog der zu verarbeitenden Daten, der automatische Abruf und die datenschutzrechtliche Kontrolle.

In der nun vorliegenden Fassung des Rundfunkgebührenstaatsvertrags ist der geforderte Katalog in § 3 Abs. 2 enthalten. Dies ist ebenso zu begrüßen wie die in Absatz 3 enthaltene Zweckbestimmung, die den Forderungen des Bundesverfassungsgerichts an bereichsspezifische Regelungen und der im neuen BDSG zum Ausdruck kommenden Tendenz entspricht. Gleichermaßen ist die in Satz 2 enthaltene Benachrichtigung des Rundfunkteilnehmers bei der automatisierten Erstspeicherung hervorzuheben.

Das Auskunftsrecht der Rundfunkanstalten gegenüber den Betroffenen (§ 4 Abs. 3) wurde in positiver Weise hinreichend präzisiert, indem die Frage, wann eine Anzeige nicht oder unvollständig erfolgt ist, an die genauen Tatbestände des § 3 Absätze 1 und 2 geknüpft wurde.

Alle vorhandenen Daten der Teilnehmer werden für die jeweils anderen Rundfunkanstalten faktisch bereitgehalten und diese sind zum Abruf berechtigt. Daß dies aus dem Text nicht deutlich wird, ist als Mangel an Transparenz zu beklagen. Die im letzten Satz geregelte Aufzeichnungspflicht enthält nicht alle Bestimmungen, die das BDSG in § 10 für die Einrichtung automatisierter Abrufverfahren trifft. Es bleibt jedoch zu hoffen, daß diese Defizite soweit möglich im Vollzug ausgeglichen werden.

Zu begrüßen ist schließlich wieder, daß nach § 8 Abs. 2 Satz 2 der betriebliche Datenschutzbeauftragte der GEZ „unbeschadet der Zuständigkeit des nach Landesrecht für die Landesrundfunkanstalt zuständigen Datenschutzbeauftragten" zu bestellen ist. Damit bleibt es den Ländern unbenommen, für den nichtjournalistisch-redaktionellen Bereich, zu dem der Gebühreneinzug gehört, die Kontrollzuständigkeit der LfD wie bereits in Hessen und Bremen vorzusehen. Dies entspricht einer Forderung, die auch von der DSK erhoben wurde. Auswirkungen für Rheinland-Pfalz ergeben sich allerdings hierdurch nicht.

Mit dem Berliner Datenschutzbeauftragten ist festzustellen, daß die Gesamtregelung den Empfehlungen aus datenschutzrechtlicher Sicht weitgehend Rechnung trägt.

18.4 Btx-Staatsvertrag

Die in § 10 des Staatsvertrags getroffene Regelung über den Datenschutz entspricht inhaltlich der bisherigen Bestimmung in Art. 9 des alten Btx-Staatsvertrages; sie entspricht im wesentlichen auch den heutigen Vorstellungen von einem wirksamen Datenschutz.

Soweit Mailbox-Systeme überhaupt unter Btx fallen, sind auch nach Auffassung des LfD die Datenschutzregelungen des Staatsvertrages für sie als nicht seitenorientierte Bildschirmtextdienste ebenfalls anwendbar.

Zu begrüßen ist die in § 2 Abs. 4 geregelte Pflicht desjenigen Anbieters, der Dritten die Möglichkeit der Verbreitung von allgemein abrufbaren Mitteilungen (sog. Pinnwände) überläßt, Anschrift und Teilnehmernummer der Dritten einen Monat lang zu speichern. Solange die Drittbenutzer anonym bleiben konnten, war manchem Unfug Tür und Tor geöffnet.

Änderungen aus der Sicht des Datenschutzes sind für den vorliegenden Entwurf nicht vorzuschlagen.

19 Telekommunikation; Telekom-Datenschutzverordnung (TDSV) und Teledienstunternehmen-Datenschutzverordnung (UDSV)

19.1 Aktueller Sachstand

Am 1. Juli 1991 ist die TDSV, eine neue Verordnung über den Datenschutz bei Dienstleistungen der Telekom in Kraft getreten. Sie umfaßt neben den Sprachkommunikationsdiensten eine Anzahl weiterer Telekommunikationsdienstleistungen. Demnächst soll eine weitgehend gleichlautende Verordnung über den Datenschutz für Teledienstunternehmen (UDSV) erlassen werden. Die darin enthaltenen Regelungen sind nur teilweise geeignet, die mit dem Einsatz der neuen Techniken einhergehenden Datenschutzprobleme zu lösen.

Umstritten war und ist insbesondere die Verarbeitung der mit der Digitalisierung der Vermittlungsstellen entstehenden Kommunikationsdatensätze, der Einzelverbindungsnachweis und die Rufnummernanzeige.

DSK und LfD haben im Jahr 1991 mehrfach in Schreiben an die Minister des Innern und für Sport sowie für Wirtschaft und Verkehr, wie auch an den Bundespostminister auf die Defizite in den beiden Datenschutzverordnungen TDSV (für Telekom) und UDSV (private Betreiber) hingewiesen. Gestützt auf das kommunikative Selbstbestimmungsrecht sowie auf das Recht auf unbeobachtbare Kommunikation wurde insbesondere gefordert:

- sofortige Löschung der für die Gebührenberechnung nicht mehr benötigten Verbindungsdaten auf Wunsch des Teilnehmers,

- beim Einzelverbindungsnachweis die generelle Verkürzung der Zielnummer um die letzten vier Ziffern,

- wahlweise, fallbezogene Möglichkeit der Unterdrückung der Rufnummernanzeige.

Im ISDN (Integrated Services Digital Network = Dienste-integrierendes digitales Fernmeldenetz) werden für jede Verbindung Datum, Uhrzeit, Dauer der Verbindung sowie Rufnummer des anrufenden und des angerufenen Anschlusses gespeichert, und zwar weit über das Verbindungsende hinaus, zumindest bis zum Versand der Entgeltrechnung, obwohl für die Gebührenberechnung die Speicherung der Ortsnetzkennzahl ausreichen würde.

Da mit der Einführung der digitalisierten Vermittlungstechnik die Arbeit derjenigen Personen und Institutionen beeinträchtigt werden kann, die in ihrer Beratungsfunktion in besonderem Maße auf die Anonymität der Kontakte angewiesen sind, hat der LfD das Ministerium für Arbeit, Soziales, Familie und Gesundheit angeschrieben, damit von dort aus die in Frage kommenden Beratungseinrichtungen bezüglich der Sicherung der Anonymität bei telefonischer Beratung informiert werden.

19.2 Anwendungsprobleme der TDSV

Die TDSV enthält durchaus einige Möglichkeiten, den geschilderten Gefahren für Beratungsstellen und diejenigen, die sie in Anspruch nehmen, entgegenzuwirken.

19.2.1 Geschützte Beratungsstellen und Einzelverbindungsnachweis

In § 6 Abs. 9 Satz 5 bis Satz 7 TDSV heißt es: „Der Anruf bei Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, darf aus dem Nachweis nicht ersichtlich sein. Hierzu gehören neben den in § 203 Abs. 1 Nr. 4 und Nr. 4 a des Strafgesetzbuches genannten Personengruppen insbesondere Telefonseelsorge und Gesundheitsberatung. Die Deutsche Bundespost Telekom ist auf Antrag einer solchen Person, Behörde oder Organisation verpflichtet, durch technische Vorrichtungen die Beachtung des Satzes 5 sicherzustellen."

Die Umsetzung dieser Regelung trifft allerdings auf erhebliche Auslegungsprobleme. So ist zunächst unklar, wer antragsberechtigt ist: Gehören zu den Antragsberechtigten auch solche Stellen, die zwar auch telefonische Beratung vornehmen, bei denen jedoch die persönliche Beratung überwiegt? Dürfen Stellen, die zwar ihre Beratungsaufgaben telefonisch wahrnehmen, bei denen aber die Beratungstätigkeit nur einen Teil ihrer Aufgaben einnimmt, Anträge stellen? Gehören auch solche Personen und Institutionen dazu, bei denen die persönliche Beratungstätigkeit telefonisch vorbereitet wird, also die telefonische Kontaktaufnahme eine wesentliche Voraussetzung für die Beratungstätigkeit ist?

Die Regelung des § 6 Abs.9 Satz 6 TDSV ist im Sinne des Datenschutzes so zu verstehen, daß – auch – solche Personen und Institutionen antragsberechtigt sind, bei denen die persönliche Beratungstätigkeit telefonisch vorbereitet wird, also die telefonische Kontaktaufnahme eine wesentliche Voraussetzung für die Beratungstätigkeit ist. Immerhin läßt sich auch aus dem Wortlaut des Satzes 6 „Hierzu gehören neben den ... insbesondere ..." entnehmen, daß die Aufzählung nicht abschließend ist.

Der Wortlaut des Satzes 5 „Der Anruf bei Personen, Behörden ... darf aus dem Nachweis nicht ersichtlich sein" läßt zwar darauf schließen, daß die Telekom selbst für die entsprechende Umsetzung Sorge zu tragen hat. Die in § 6 Abs. 9 Satz 7 geregelte Verpflichtung der Telekom, auf Antrag durch einen Berechtigten tätig zu werden, bleibt jedoch hiervon unabhängig. Ferner ist unklar, wie weit das Prüfungsrecht der Telekom bzw. der Teledienstunternehmen geht, insbesondere welche Informationen die Antragsteller beizubringen haben.

Weiterhin ist nicht ersichtlich, wie bei Anschlüssen von Personen, Organisationen und Behörden verfahren werden soll, die an betriebliche Nebenstellenanlagen angeschlossen sind, insbesondere ob die Sperre einzelner Nebenstellennummern im Einzelentgeltnachweis möglich ist.

19.2.2 Rufnummernanzeige

Die Vorschriften über die Rufnummernanzeige sind wesentlich klarer gefaßt:

§ 9 Abs. 1 Satz 2 TDSV verpflichtet die Telekom, dem Kunden die Wahlmöglichkeit zwischen der Anzeige seiner Rufnummer bei jedem Anruf und dem Ausschluß der Rufnummernanzeige beim Angerufenen auf Dauer einzuräumen.

§ 9 Abs. 1 Satz 3 enthält folgende Regelung: „Für Sprachkommunikationsdienste ist auf Antrag die Übermittlung der Rufnummer des anrufenden Anschlusses an den angerufenen Anschluß einer der in § 6 Abs. 9 Satz 5 genannten Personen, Organisationen und Behörden in der Vermittlungsstelle dieses Anschlusses auszuschließen."

Der LfD hat gegenüber dem Ministerium für Arbeit, Soziales, Familie und Gesundheit angeregt, durch geeignete Maßnahmen sicherzustellen, daß die in Frage kommenden Beratungseinrichtungen bei den jeweiligen Fernmeldeämtern beantragen, auf dem Einzelentgeltnachweis nicht zu erscheinen und sich von der Rufnummernübermittlung ausschließen zu lassen. Ferner hat er

dabei auf folgendes hingewiesen: Während der Ausschluß der Rufnummernanzeige gem. § 9 seit dem Inkrafttreten der TDSV am 1. Juli 1991 bereits möglich ist, tritt die Regelung des § 6 Abs. 9 Satz 5 (Einzelentgeltnachweis) erst in Kraft, sobald die zu ihrer Durchführung erforderlichen DV-Programme verfügbar sind, spätestens am 1. Juli 1992. Dies bedeutet, daß in der Zwischenzeit sämtliche Anrufe, also auch solche bei den „geschützten" Personen, Behörden und Organisationen auf dem Einzelentgeltnachweis ersichtlich sind. Durch die gegenwärtig bestehende praktische Unmöglichkeit der Unterdrückung eines solchen Anrufes auf dem Entgeltnachweis ist der Schutzzweck der Regelung insoweit in Frage gestellt.

Schließlich hat der LfD angemerkt, daß die Antragstellung gem. § 9 Abs. 1 Satz 3 TDSV auch dann sinnvoll ist, wenn – noch – keine digitalisierten Telefonanlagen installiert sind; denn nur wenn entsprechende Anträge gestellt sind, wird im Telefonbuch vermerkt, daß keine Rufnummernanzeige stattfindet und der Anrufer kann sicher sein, anonym zu bleiben.

19.3 Parallelprobleme der UDSV

Im Hinblick auf die Beratungen der UDSV im Bundesrat wurde das Ministerium des Innern erneut von der Entschließung der Datenschutzbeauftragten des Bundes und der Länder in Kenntnis gesetzt. Dabei wurden die wesentlichen Defizite des Entwurfs aufgezeigt und um Unterstützung der Forderungen im Bundesrat gebeten. In folgenden Bereichen wurden die Forderungen der Entschließung der Datenschutzbeauftragten nicht berücksichtigt:

Nach § 6 Abs. 1 UDSV-E dürfen sämtliche Verbindungsdaten entgegen der Forderung der Datenschutzbeauftragten zur Entgeltermittlung von den Unternehmen vollständig gespeichert werden.

§ 6 Abs. 2 enthält nur für die Sprachkommunikationsdienste ein Wahlrecht des Kunden über die Datenspeicherung für die Zeit nach der Versendung der Entgeltrechnung. In sämtlichen anderen Diensten dürfen die Verbindungsdaten stets bis zu achtzig Tage nach Versendung der Entgeltrechnung gespeichert bleiben.

§ 6 Abs. 9 erlaubt den Unternehmen, ihren Kunden auf Antrag ausführliche Einzelentgeltnachweise mit unverkürzten Rufnummern zur Verfügung zu stellen. Ausnahmen sind lediglich für Anrufe bei „Personen, Behörden und Organisationen, die selbst oder deren Mitarbeiter besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln" vorgesehen. Auch hierfür gelten die obigen Ausführungen zum Schutz der Anonymität bei telefonischer Beratung.

Bei Anrufen wird am angerufenen Apparat die Rufnummer des anrufenden Anschlusses angezeigt. Diese Rufnummernanzeige kann entgegen der Forderung der Entschließung nur generell, nicht aber fallweise „auf Knopfdruck" unterdrückt werden. Die Möglichkeit zur fallweisen Unterdrückung durch den Anrufer ist erst zum 1. Januar 1994 vorgesehen; der Angerufene kann die Rufnummernanzeige überhaupt nicht fall- oder zeitweise abschalten und muß sich zwischen Anschlüssen mit oder ohne Anzeige entscheiden. Auch in diesem Bereich ist wiederum eine bedenkliche zeitliche Schutzlücke vorhanden.

Der Entwurf trägt damit den datenschutzrechtlichen Anforderungen an eine Regelung über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Zusammenhang mit der Erbringung von Telekommunikationsdienstleistungen durch Teledienstunternehmen nicht genügend Rechnung.

19.4 Offene Fragen

Es ist darauf hinzuweisen, daß beide Verordnungen nicht nur den ISDN-Teilnehmer, sondern gemäß § 1 Abs.1 Satz 1 TDSV/UDSV alle am Fernmeldeverkehr Beteiligten betreffen.

In diesem Zusammenhang stellt sich die Frage, wie es um den Schutz des mit analoger Technik ausgestatteten Teilnehmers bestellt ist. Zum Beispiel sollte der Verordnungsgeber klarstellen, ob die Rufnummer eines „analogen Anrufers", der über eine digitalisierte Vermittlungsstelle mit einem „digitalen Angerufenen" Kontakt aufnimmt, dort auf dem Display angezeigt wird. Von der Technik her ist dies möglich. Wenn die Anzeige softwaremäßig verhindert wird, sollte eine entsprechende Handhabung in den Datenschutzverordnungen ihren Niederschlag finden, damit sich der analoge Teilnehmer im Falle der Nichteinhaltung darauf berufen kann.

Ferner ergibt sich aus den Verordnungen nicht eindeutig, ob auch der mit einer digitalisierten Vermittlungsstelle verbundene analoge Teilnehmer Anspruch auf den Einzelverbindungsnachweis hat. Sollte er nicht in den „Genuß" dieser Abrechnungsart kommen können, so wäre eine entsprechende Klarstellung angebracht.

Weiterhin wäre wünschenswert, daß auch der analoge Anrufer in die Lage versetzt wird, fallbezogen zu entscheiden, ob seine Rufnummer dem mit digitaler Technik ausgestatteten Angerufenen angezeigt wird; etwa durch Vorwahl einer bestimmten Zahlenfolge, die dann in der – digitalisierten – Vermittlungsstelle dem Wunsch des Anrufers entsprechend umzusetzen ist.

Zudem sollte man über die aktuelle Forderung der fallweisen Rufnummernunterdrückung hinaus einen Blick auf die wohl richtungsweisende Entwicklung in den USA werfen. Dort hat sich ein sinnvoller Interessenausgleich zwischen dem Anrufer und dem Angerufenen durchgesetzt, der die fallbezogene Unterdrückungsmöglichkeit bei den Anrufenden mit einer damit korrespondierenden möglichen Sperre für nicht identifizierte Anrufe bei den Angerufenen koppelt. Für diese Technik wurde der Begriff „Blocking" geprägt. Übrigens beinhaltet der von der EG-Kommission vorgelegte Entwurf eines „Vorschlags für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im dienste-integrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" in Artikel 12 ebenfalls die Möglichkeit einer solchen Sperre. Danach muß der angerufene Teilnehmer die Entgegennahme ankommender Verbindungen auf diejenigen beschränken können, bei denen die Nummer des anrufenden Teilnehmers angegeben ist. Seine optimale Ausgestaltung würde das Recht auf kommunikative Selbstbestimmung in diesem Bereich allerdings erst dann erfahren, wenn für den Angerufenen die Wahlmöglichkeit bestünde, sein Telefon so einzustellen, daß nur identifizierte Anrufe akzeptiert werden und im Falle des nicht erkennbaren Anrufers dieser automatisch zur Eingabe seiner Identität aufgefordert wird. Eine derartige – gebührenfreie – Dialoglösung wird als „Handshaking" bezeichnet und kann aus der Sicht des Datenschutzes als Beispiel einer dem kommunikativen Selbstbestimmungsrecht Rechnung tragenden datenschutzgerechten Technikgestaltung angesehen werden.

19.5 Teilerfolge des Datenschutzes

Die massive Kritik des Datenschutzes hat den praktischen Umgang der Telekom mit der TDSV offenbar bereits im positiven Sinne beeinflußt. Wie zu erfahren war, wurden seit dem Inkrafttreten der TDSV Einzelverbindungsnachweise noch nicht erstellt, vielmehr die Einführung bundesweit zurückgestellt (Stand: September 1991). Allem Anschein nach wird bei der Telekom über eine andere Ausgestaltung des Einzelverbindungsnachweises nachgedacht. So ist gegenwärtig ein Modell in der Diskussion, das eine allgemeine Kennung für Anrufe bei Ansagediensten vorsieht (Auskunft, Zeitansage, Sportnachrichten, Kinoprogramme, Zahlenlotto, Fußballtoto, Veranstaltungshinweise usw.), unter die dann auch der Anruf bei einer geschützten Beratungsstelle fallen könnte. Es steht zu hoffen, daß diese Entwicklung zu weiteren wünschenswerten Verbesserungen des Schutzes personenbezogener Daten führt.

20 Technischer und organisatorischer Datenschutz

20.1 Allgemeines

Die in den vorangegangenen Tätigkeitsberichten der DSK geäußerten Erwartungen, daß sich die rasante Entwicklung der Computertechnik und der Einsatz immer leistungsfähigerer Geräte beschleunigen werde, hat sich bestätigt. Wurden in der Vergangenheit noch bei Datenverarbeitungsanlagen in einer Behörde die Arbeitsplätze mit sogenannten „unintelligenten" Bildschirmen ausgestattet, so sind es heute überwiegend PC, die angeschlossen werden. Gleiches gilt auch für Anschlüsse an das rheinland-pfälzische Datenkommunikationsnetz (vgl. Tz. 20.4). Solange sich die Automatisierte Datenverarbeitung im wesentlichen auf den Einsatz von Online-Verfahren beschränkte, hielten sich die Datensicherungsprobleme auf der Ebene der Übermittlungsempfänger in Grenzen. Mit der Einrichtung autonomer PC-Arbeitsplätze und dem Aufbau vernetzter Systeme hat sich die Situation verändert. Beratungs- und Kontrollnotwendigkeiten entstehen in weitaus stärkerem Umfange als früher an den Stellen, die unter Verwendung intelligenter Systeme auf zentrale Datenbanken zugreifen. Ohne einen zusätzlichen Mitarbeiter im Referat für technisch-organisatorische Datenschutzangelegenheiten sind diese Aufgaben nicht mehr angemessen zu erfüllen.

Im Blick auf den verstärkten Einsatz intelligenter Datenendgeräte und von Arbeitsplatzrechnern bestand die Notwendigkeit, die Orientierungshilfe zu datenschutzrechtlichen Sicherungsmaßnahmen – Heft 2 der Schriftenreihe „Informationen zum Datenschutz" – um spezielle Hinweise auf die technischen und organisatorischen Datenschutzanforderungen zu ergänzen.

Örtliche Feststellungen im Berichtszeitraum ergaben, daß in Verwaltungen, in denen keine zentrale Zuständigkeit für Fragen des geordneten PC-Einsatzes und für technische und organisatorische Datenschutzmaßnahmen besteht, häufig gravierende Mängel zu beklagen waren. Anmeldungen zum Datenschutzregister unterblieben, die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten wurde nicht geprüft und Dienstanweisungen nach § 9 LDatG nicht erlassen. Das Interesse der Verantwortlichen war oft nur auf das Erreichen eines stabilen Betriebszustandes gerichtet, während die Frage, welche Datensicherungsmaßnahmen angemessen seien, oft ungeprüft blieb.

Die Datenschutzbeauftragten des Bundes und der Länder sowie die DSK Rheinland-Pfalz haben in ihrer Entschließung vom 10. Oktober 1988 (vgl. 11. Tb, Tz. 19.2) auf die besonderen Gefahren beim Einsatz von kleineren Datenverarbeitungsanlagen und insbesondere beim PC-Einsatz hingewiesen. Die Aufforderungen an die Hersteller von Hard- und Software, Verfahren zu entwickeln, die beim Betrieb dieser Geräte ein Maß an Datensicherheit ermöglichen, das dem großer Rechenzentren entspricht, wurden mittlerweile in befriedigendem Maße umgesetzt.

Die DSK und der LfD haben in der Vergangenheit den Einsatz spezieller Sicherungsprodukte stets dann gefordert, wenn sensible Daten verarbeitet werden sollen und auf andere Weise ein angemessener Datenschutz nicht zu erreichen ist (vgl. a. a. O. Tz. 19.3).

Obwohl leistungsfähige Sicherheitsprodukte erhältlich sind und deren Kosten nur bei ca. 5 % des Anschaffungspreises des Systems liegen, ist gerade im kommunalen Bereich festzustellen, daß diese Produkte nicht eingesetzt werden, obwohl z. B. im Sozialamt, im Jugendamt oder im Personalamt besonders sensible Daten gespeichert werden. Nach wie vor fehlt es im gemeindlichen Bereich an Beratung in Fragen der Gerätebeschaffung und zur Lösung programm- und systemtechnischer Probleme. Die Beratung des LfD und seiner Mitarbeiter wird in Anspruch genommen, umfaßt aber, entsprechend seiner Aufgabenstellung, nur den engeren Bereich des technischen und organisatorischen Datenschutzes.

Für den Bereich der Landesregierung hat der Ministerrat auf der Grundlage der Studie eines Beratungsunternehmens die Durchführung eines Pilotprojektes zur ressortübergreifenden Bürokommunikation beschlossen. Diese soll in der Staatskanzlei, im Ministerium des Innern und für Sport sowie im Ministerium für Wirtschaft und Verkehr getestet und bis Ende 1992 in Betrieb genommen werden. Die Studie wurde dem LfD zur Kenntnisnahme vorgelegt. Eine Beurteilung aus datenschutzrechtlicher Sicht setzt voraus, daß ein Datenschutz-/Datensicherheitskonzept erstellt wird, aus dem die Rechtsgrundlagen für die Erhebung, Übermittlung und Löschung von Daten, der Umfang der Daten und der betroffene Personenkreis sowie Maßnahmen zur Gewährleistung der Datensicherheit ersichtlich sind. Ferner sind die Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IT-Mindestanforderungen 1990) zu berücksichtigen. Die Aussage in der Ministerratsvorlage, daß die Belange des Datenschutzes berücksichtigt werden, ist ohne Kenntnis der Details eines Sicherheitskonzepts für den LfD zur Zeit nicht verifizierbar.

20.2 Risiken beim Einsatz von Laptops

Die bereits aus der Anwendung von PC bekannten Risiken werden beim Einsatz von Laptops außerhalb einer Behörde dadurch verstärkt, daß die in der herkömmlichen Büroumgebung getroffenen Sicherungsmaßnahmen (Zugang zu den Geräten, Sicherheitsschlösser, Schließanlage usw.) wegfallen. Dies hat zur Folge, daß bei Unachtsamkeit der Besitzer beispielsweise die Gefahr des Diebstahls groß ist. Für die Zugriffssicherheit von Laptops, auf denen besonders sensible personenbezogene Daten gespeichert werden, gilt das gleiche wie bei der Verarbeitung auf PC: Ohne eine spezielle Sicherungssoftware oder Hardware, die geeignet ist, den unberechtigten Datenzugang zu verhindern, darf ein Laptop nicht eingesetzt werden.

Eine weitere Gefahr liegt darin, daß durch Anwendung fehlerhafter Software (beisp. virenbehaftete Programme) bei der Datenübertragung in stationäre Systeme Daten verloren gehen oder andere Fehler entstehen. Da die gespeicherten Daten auf Laptops oftmals auf stationäre Systeme mit den zur Verfügung stehenden Kommunikationsschnittstellen über Modem, Akustikkoppler oder über ein Rechnerverbundnetz übertragen oder in der entgegengesetzten Richtung abgezogen werden, besteht auch die Möglichkeit, daß dies unbefugt geschieht, da die Anzahl der Netzteilnehmer unüberschaubar wird.

Um eine angemessene Datensicherheit bei der Verarbeitung von personenbezogenen Daten auf Laptops zu gewährleisten, sollten beim Einsatz solcher Geräte die nachfolgenden Vorkehrungen getroffen werden.

Organisatorische Maßnahmen:

- Auswahl und Beschaffung der Geräte, Installation der Anwendungsprogramme sowie der Sicherungssoftware und Hardware durch eine zentrale Stelle (Benutzerservice); Sicherheitsausstattung (Tastaturschloß, Gehäuseschloß, verschließbares Behältnis für die Aufbewahrung des Laptop);

- Regelung der Verantwortlichkeit für die Geräte und ihre Wartung;

- Regelungen über die Aufbewahrung der Geräte nach Dienstschluß oder bei Dienstreisen;

- Anweisung, nur freigegebene Programme einzusetzen und diese nur in compilierter (unveränderlicher) Form zu speichern;

- Bestimmung der für die Kontrolle der Geräte zuständigen Personen (z. B. Überprüfung von Protokolldateien);

- Schriftliche Regelungen über Art und Umfang des Laptop-Einsatzes in einer Dienstanweisung (§ 9 LDatG).

Technische Maßnahmen:

- Die Geräte sind mit einer Sicherheitssoftware und Hardware auszustatten, die eine Authentisierung (Benutzer) und Autorisierung (Zugriffsrechte) voraussetzt.

- Die Benutzung des Laptop ist maschinell zu protokollieren. Die Überprüfung der Protokolldateien sollte nur von einer hierfür beauftragten Person (z. B. Datenschutzbeauftragter, Benutzerservice) und zentral in der Dienststelle möglich sein.

- Um Hardwaremanipulationen zu vermeiden, sollte das Gehäuse des Rechners durch geeignete Maßnahmen (z. B. Versiegeln, Verplomben) gesichert werden.

- Nicht benötigte Kommunikationsschnittstellen sind außer Betrieb zu setzen.

- Wird das Gerät von mehreren Bediensteten genutzt, ist für jeden Benutzer ein Benutzername (User-id) und ein Paßwort einzurichten. Die Paßwörter sollten verschlüsselt gespeichert werden.

- Um zu verhindern, daß beim Start des Betriebssystems über das Diskettenlaufwerk die installierte Sicherheitssoftware umgangen wird, sollte das Diskettenlaufwerk gesperrt werden. Somit kann verhindert werden, daß Programme und Daten eingespeichert werden, die für die Aufgabenerfüllung nicht erforderlich sind, und unbefugt Daten kopiert werden.

- Bei besonders schutzwürdigen Daten muß die Verschlüsselung festgelegter Datenbestände oder der gesamten Festplatte möglich sein.

- Eine Zugriffsberechtigung auf die Betriebssystemebene sollte nur für den Systemverwalter zugelassen werden. Der Befehlsumfang sollte durch die Sicherungssoftware gesteuert werden. Zugriffe sind in der Logdatei aufzuzeichnen.

Mit diesen Maßnahmen kann zwar die Datensicherheit erhöht, aber kein vollständiger Schutz erzielt werden. Die Mitarbeiter, die solche Geräte einsetzen, sollten besonders auf die Anwendungsrisiken hingewiesen und auf die strikte Einhaltung der Datensicherheitsvorschriften verpflichtet werden.

Ist eine ausreichende Sicherheit nicht zu erreichen, muß auf den Einsatz eines Laptop verzichtet werden.

20.3 „Viren" in DV-Systemen

Aus Presseberichten konnte man in der Vergangenheit häufig Warnungen entnehmen, daß der Virenbefall von Personalcomputern ständig steigen wird. Die These, daß 1994 20 v. H. aller Personalcomputer in der Bundesrepublik von Viren befallen seien, und die Zahl der heute bekannten Virenarten um ca. 50 v. H. zunehmen werde, wird von Experten bestätigt.

Festzustellen ist, daß die Viren – dies sind spezielle Programme zur (ungewollten) Daten-Zerstörung – immer aggressiver, ihre Tarnung immer besser wird, und daß sie bei Programmen und Datenbeständen enorme Schäden anrichten können. Inzwischen gibt es auf dem Softwaremarkt eine Vielzahl von Programmen, die bei der Erkennung und Bekämpfung unterschiedliche Dienste leisten. Die Viren-Bekämpfer können indessen mit ihren Erkennungs- und Bekämpfungsprogrammen kaum mehr mit der Virenprogrammierung Schritt halten. Waren früher ein von zwanzig Virenprogrammen wirklich gefährlich, so ist schon jetzt jede zweite Virusart so entwickelt, daß sie Programme und Datenbestände zerstören.

Im Berichtszeitraum wurden Fälle des Virenbefalls in PC an Arbeitsplätzen in der öffentlichen Verwaltung festgestellt. Ursachen der Infizierung waren kopierte Spielprogramme und infizierte Anwendungsprogramme, die ein Softwarehaus ohne Kenntnis der Infizierung weitergab.

Werden solche Fälle bekannt, sollten unverzüglich folgende Maßnahmen eingeleiten werden:

- Gerät ausschalten und alle Kommunikationsverbindungen unterbrechen„

- bei PC, die mit einer Batteriepufferung arbeiten, sollten die Batterien ausgebaut und der PC solange außer Betrieb genommen werden, bis von einer vollständigen Löschung aller Informationen ausgegangen werden kann (ein bis zwei Tage);

- PC mit der schreibgeschützten Originalbetriebssystemdiskette neu starten;

- die infizierten Programme zu Beweiszwecken sichern;

- die Festplatte und alle betroffenen Datenträger neu formatieren;

- vor Installation der Anwendungssoftware und Dateien (Backup) sollten diese mit einem Virensuchprogramm auf Virenbefall untersucht werden.

Zum Schutz vor Computerviren sollten folgende Sicherheitsmaßnahmen beachtet werden:

- kein Einsatz von Raubkopien, insbesondere von Spielprogrammen;
- keine Verwendung von privater Hard- und Software;
- kein Einsatz von PUBLIC-DOMAIN-Software;
- kein Einsatz fremder, nicht geprüfter und freigegebener Software;
- Einsatz von Virensuchprogrammen zur Überprüfung von Programmen und Dateien, die über Modem und Netzwerk geladen werden;
- besondere Sicherung der Quellprogramme, wenn diese im Quellcode gespeichert werden;
- Umbenennung ausführbarer Programme (COM, EXE, BAT), damit diese nicht aufgefunden und infiziert werden können.

Zur Entdeckung und zum Schutz vor Viren bieten einige Softwarehersteller heute Schutz- und Analyseprogramme an. Ein solches Programm sollte

- die bekanntesten Viren an ihrer Signatur erkennen;
- vor der Installation den Speicher des Rechners und den Bootsektor nach Virenbefall überprüfen;
- alle Programme, die über Diskette, Modem und Netzwerk geladen werden, überprüfen;
- die speicherresidenten Programme überwachen und
- bei der Prüfung ein manipulationssicheres Verfahren wählen.

20.4 Datenschutz und Datensicherheit für die Nutzung des rheinland-pfälzischen Datenkommunikationsnetzes

In der Vergangenheit wurden im rheinland-pfälzischen Datenkommunikationsnetz primär „unintelligente" Endgeräte (Bildschirme/Drucker) eingesetzt. Soweit diese Geräte vor Ort durch das Landesrechenzentrum eingerichtet wurden, war eine eindeutige Zuordnung der physischen Geräte zu einem logischen Netzwerknamen gewährleistet. Hierbei beinhaltete der Netzwerkname die Behörde (Stadtverwaltung), den funktionellen Bereich (Einwohnermeldeamt, Ordnungsamt usw.) und den Standort der Geräte (Stadt-/Ortsname). Eingriffsmöglichkeiten von seiten der Anwender bestanden praktisch nicht; der gerätebezogene Netzwerkname reichte für die Regelung der Zugangssicherung, Zugriffsberechtigung und der Kontrolle des Netzes aus, wenn das angeschlossene Endgerät von einer Person genutzt wurde. Da heute in zunehmendem Maße die Anforderung besteht, Arbeitsplatzrechner (PC), vernetzte Arbeitsplatzrechner, Behörden-/Abteilungsrechner oder Zentralrechner an das Kommunikationsnetz anzuschließen, bietet die noch gerätebezogene Zugangsberechtigung nach Auffassung der DSK und des LfD nach dem heutigen Stand der Technik keine ausreichende Datensicherheit mehr. Dies hat zur Folge, daß durch den Einsatz der genannten Rechnersysteme die bisher gegebene eindeutige Zuordnung von Geräten und Netzwerknamen unterlaufen werden kann. Durch diese Anschlußmöglichkeit von Datenendgeräten (PC oder Bildschirme) an ein System vernetzter Arbeitsplatzrechner oder einen mehrplatzfähigen Behörden-/Abteilungsrechner, verliert das für die Kommunikation und Anwendung zuständige Rechenzentrum (LRZ) die Möglichkeit einer umfassenden Netzwerk-Kontrolle. Eine Verstärkung dieser Problematik ergibt sich daraus, daß mehrere Verwaltungen einen einzigen Rechner für den Zugang zum Datenkommunikationsnetz nutzen und damit eine Trennung der Zugriffsberechtigungen durch die Netzwerknamen nicht sichergestellt werden kann. Ein weiteres Risiko liegt darin, daß angeschlossene Rechnersysteme zusätzlich über Wählleitungsanschlüsse verfügen können, deren Vorhandensein dem netzbetreibenden Rechenzentrum nicht bekannt sind bzw. von ihm nicht beeinflußt werden können.

In ihrem 12. Tätigkeitsbericht (Tz. 19.6) hatte die DSK für die Zugriffe auf das landeseinheitliche EWOIS-Verfahren bereits gefordert, daß bei der Datenübermittlung und bei Online-Zugriffen eine Authentisierung (Benutzer, Datenstation) und Autorisierung (Zugriffsrechte) realisiert wird. Dies ist notwendig, um eine höhere Verfahrenssicherheit zu erreichen und um die Voraussetzungen nach § 9 Abs. 1 Nr. 7 LDatG (Eingabekontrolle) zu erfüllen. Vor diesem Hintergrund und angesichts der weiteren technischen Entwicklung haben die DSK und der LfD die Thematik im Berichtszeitraum mehrfach mit den verantwortlichen Mitarbeitern des LRZ erörtert. Das Ergebnis dieser Erörterungen veranlaßte die DSK, das Ministerium des Innern um Prüfung zu bitten, in welcher Weise eine dem heutigen Stand der Technik entsprechende Datensicherheit erreicht werden kann. Eine von der DSK angeregte und vom Ministerium des Innern eingesetzte Arbeitsgruppe wurde beauftragt, die Schutzmechanismen des

Datenkommunikationsnetzes zu überprüfen und DV-technische und organisatorische Überlegungen zur Gewährleistung der Sicherheit aufzuzeigen. Nach Auffassung der Arbeitsgruppe ist für die Entwicklung eines umfassenden Konzeptes zur Gewährleistung der Datensicherheit im Netz von folgenden Grundsätzen auszugehen:

- Einrichtung und Betrieb der Netze müssen so erfolgen, daß jederzeit die Erfüllung aller datenschutzrechtlich und geheimhaltungsrechtlich relevanten Vorschriften (z. B. LDatG, BDSG, Statistikgesetze oder sonstige bereichsspezifische Regelungen) gewährleistet sind.

- Das Datenschutz- und -sicherheitskonzept muß ein einheitliches, systematisches, vollständiges und geschlossenes System (Recht, Organisation und Technik) bilden: Das Konzept des Netzzugangs muß alle Anwendungen abdecken, d. h., die datenschutzrechtlich relevanten wie auch die übrigen Anwendungen. Darüber hinaus muß das Konzept für alle Benutzer bzw. Benutzergruppen in gleicher Weise gelten.

- Der Zugang zum Datennetz muß einerseits nach Verwaltungen und Verwaltungsgruppen sowie andererseits innerhalb einer Verwaltung oder Verwaltungsgruppe differenzierbar sein. Anzuknüpfen ist an den dem Datenschutz zugrundeliegenden funktionalen Behördenbegriff.

- Das Konzept muß im Rahmen der Administration des Netzzugangs eine verteilte Zuständigkeit und Verantwortlichkeit für unterschiedliche Aufgaben der Fachaufsicht, Rechenzentren und Endbenutzerverwaltungen vorsehen. Die Zuständigkeiten zur Administration der Netzwerksicherheit sind in einer allgemein verbindlichen Benutzerordnung festzuschreiben.

- Es muß erkennbar sein, von welcher Verwaltung (Typ und Ort) und von welchem funktionalen Bereich innerhalb der einzelnen Verwaltung ein Netzzugang erfolgt.

- Die Benutzung des Netzes und die Übermittlung von Daten müssen in geeigneter Weise protokolliert werden. Die Protokolle müssen eine nachträgliche Auswertung und Überprüfung (z. B. durch den Datenschutzbeauftragten) sicherstellen.

- Es muß sichergestellt sein, daß der Zugang zum Netz nur benutzerbezogen bzw. benutzer- und gerätebezogen möglich ist. Den Benutzern zentraler DV-Verfahren darf nur der Zugang zu und die Nutzung von solchen Verfahren bzw. Verfahrensteilen möglich sein, für die eine explizite Berechtigung besteht.

- Der Zugang zum Netz muß über mehrere Stufen geregelt sein: Zugang zum Landesdatennetz, Zugang zu Trägersystemen (z. B. Datenbanksystem IMS oder DB2), Zugang zu DV-Verfahren oder DV-Verfahrensteilen.

- Alle einem Arbeitsplatz zugeordneten und aktivierbaren Funktionen sind bei Nichtbenutzung zeitlich zu limitieren.

- Für die Vergabe von Paßwörtern und für die Behandlung von Fehlversuchen müssen restriktive Regeln gelten.

Nachdem die Beratungsergebnisse der Arbeitsgruppe seit geraumer Zeit dem Ministerium vorliegen, ohne daß etwas geschehen ist, hat der LfD die Realisierung angemahnt.

20.5 Datensicherheit beim Einsatz von UNIX-Systemen

Nach den im Rundschreiben des Ministeriums des Innern vom 15. Mai 1990, MinBl. 1990, S. 166 „Automatisierte Datenverarbeitung in der Landesverwaltung Rheinland-Pfalz" enthaltenen Standards soll das Betriebssystem MS-DOS für Einplatzsysteme und UNIX für Mehrplatzsysteme eingesetzt werden. Mit diesen Festlegungen soll gewährleistet werden, daß in der Landesverwaltung möglichst einheitliche und wirtschaftliche Hardware eingesetzt und die Portabilität standardisierter Software ermöglicht wird.

Diese Anforderungen wurden auch der Ausschreibung eines Bürokommunikationssystems für die Geschäftsstelle der DSK zugrunde gelegt. Die Geschäftsstelle ist seit einem Jahr mit einem UNIX-System ausgestattet und konnte in dieser Zeit entsprechende Erfahrungen bezüglich der Datensicherheit solcher Systeme sammeln, die sich in diesem Bericht wiederfinden.

Für die ursprünglichen Betriebssystemversionen, die überwiegend im technischen und wissenschaftlichen Bereich eingesetzt wurden, standen sicherlich nicht die Sicherheitsanforderungen an erster Stelle. Da UNIX inzwischen auf dem Weg zum Standardbetriebssystem ist, das Anwendungsbereiche jeglicher Art abdeckt, wurde mit den neueren Versionen ein vertretbarer Sicherheitsstandard erreicht, der eine Verbesserung der Zugriffssicherung und der Absicherung der Benutzer beinhaltet.

Ist bei dem Betriebssystem MS-DOS eine Zugriffskontrolle nur durch zusätzliche Sicherungssoftware und Hardware möglich, ist das Betriebssystem UNIX standardmäßig mit Zugriffskontroll- und Protokollierungsmöglichkeiten ausgestattet. Durch die

Möglichkeit, daß mehrere Benutzer gleichzeitig am System arbeiten und unterschiedliche Programme nutzen können, z. B. Zugriffe auf Datenbanken vornehmen, Texte schreiben und Dokumente ausdrucken können, sind komplexe Zugriffsprofile für Benutzer zu erstellen, die Manipulationen weitgehend ausschließen.

Der Zugriff bei UNIX erfolgt standardmäßig mit der Eingabe des zugelassenen Benutzernamens und eines individuellen, bei der Eingabe nicht angezeigten Paßwortes zur Authentifikation. Der Benutzer muß zuvor durch den Systemverwalter oder Administrator mit seinen Berechtigungen in einer LOGIN-Datei eingetragen werden. Die Paßwörter werden in einer Datei in verschlüsselter Form gespeichert und können auch vom Systemverwalter nicht entschlüsselt werden. Hat ein Benutzer sein Paßwort vergessen, kann der Systemverwalter dieses entfernen und durch ein anderes ersetzen. Festlegungen über eine Mindestlänge und die Vorgabe für den Verfall von Paßwörtern sind in den auf dem Markt befindlichen UNIX-Systemen unterschiedlich realisiert; sie gehören nicht zum Standard von UNIX.

Die einfachste Möglichkeit, sich unbefugt Zugang zum System zu verschaffen, besteht darin, daß ein Paßwort durch ständig neue Anmeldeversuche erraten wird. Ein Mangel ist sicherlich, daß das System beliebige Fehlversuche zuläßt, ohne daß eine Sperrung des Eingabegerätes oder der Benutzerkennung erfolgt.

Für jeden Benutzer sollte geprüft werden, ob er über eine Shell-Berechtigung (Aufruf der Betriebssystemebene) verfügen muß. Mit einer Shell-Berechtigung und Kenntnis des Paßwortes ist bei Eingabe des „SU"-Kommandos (Super-User) die Möglichkeit gegeben, die Funktionen des Systemverwalters „root" zu nutzen. Weiterhin besteht die Möglichkeit, daß der Shell-Berechtigte mit der Kommandosprache des Betriebssystems oder mit der Programmiersprache C Programme erstellen, Programme aufrufen und Betriebssysteminformationen anfordern kann.

Der Systemverwalter in UNIX-Systemen hat Zugriffsrechte auf sämtliche Ressourcen, kann alle Dateien lesen und verändern, Eigentums- und Zugriffsrechte verändern, Systeminformationen manipulieren, Paßworttabellen bearbeiten, Benutzer hinzufügen, sperren und deren Berechtigungen verändern. Diese umfassenden Berechtigungen des Systemverwalters sind nicht kontrollierbar, da er selbst auch die Möglichkeit hat, Systemprotokolle zu verändern und zu löschen. Durch diese weitreichenden Berechtigungen, die für die Systemverwaltung unter UNIX sehr nützlich sind, ergeben sich jedoch Probleme für den Datenschutz und die Datensicherheit. Die Auswahl und Qualifizierung eines befähigten und zuverlässigen Systemverwalters und mindestens eines ebenso befähigten und zuverlässigen Vertreters sollte die Grundvoraussetzung für eine sichere Anwendung sein. Wegen der vorgenannten Risiken in der Systemverwaltung empfiehlt der LfD, beim Einsatz von UNIX-Systemen die Möglichkeit der Funktionstrennung zu nutzen. So sollte der Systemverwalter der EDV-Abteilung oder dem Benutzerservice zugeordnet sein und nicht selbst Anwenderaufgaben wahrnehmen. Eine weitere Sicherheit bietet auch die Möglichkeit, daß ein geteiltes Paßwort vergeben wird und somit eine Anmeldung im System nach dem Vieraugenprinzip nur von zwei Personen gemeinsam erfolgen kann. Eine ausreichende Schulung der Systemverwalter sollte vor der Installation und Einrichtung des Systems vorgenommen werden, da gerade bei der Installation Sachkenntnis und Sorgfalt unabdingbar sind.

Aufgrund der starken Verbreitung von UNIX ist zu erwarten, daß zukünftig von den Anwendern immer höhere Anforderungen an die Sicherheit der Systeme gestellt werden. So bieten schon jetzt diverse Softwarehäuser über den Standard hinausgehende Zusatzprodukte an, die die genannten Risiken für den Zugriffsschutz auf Benutzerebene, auf Dateien und für die Systemverwaltung ausschließen.

20.6 Ergebnisse örtlicher Feststellungen

Beauftragte der DSK und des LfD haben im Berichtszeitraum bei einer Kreisverwaltung sowie mehreren Stadt- und Gemeindeverwaltungen örtliche Prüfungen mit dem Schwerpunkt „technische und organisatorische Datenschutzmaßnahmen" durchgeführt. Aus den Feststellungen und Empfehlungen sind im folgenden nur solche dargestellt, die in diesem Bericht nicht bereits unter dem Gesichtspunkt der allgemeinen Datensicherheit angesprochen wurden.

20.6.1 Datenschutzbeauftragter; zentrale Datenschutzstelle

Aufgrund der Verweisung in § 79 SGB X auf Vorschriften des BDSG sind Sozialleistungsträger verpflichtet, einen Beauftragten für den Datenschutz zu bestellen, wenn ein bestimmtes Mindestquorum bei der Datenverarbeitung regelmäßig und ständig beschäftigter Personen erreicht ist (5 Personen bei automatisierter Datenverarbeitung, 20 Personen bei manueller Dateiführung). Die gleiche Verpflichtung besteht für öffentlich-rechtliche Wettbewerbsunternehmen aufgrund der Verweisung in § 2 Abs. 4 LDatG. Die örtlichen Feststellungen ergaben, daß dieser Verpflichtung nicht immer entsprochen wurde. Gelegentlich war zwar ein Datenschutzbeauftragter bestellt, der indessen in diesem Arbeitsgebiet noch keinerlei Aktivität entfaltet hatte.

Es zeigte sich im übrigen, daß es für die Verwaltung von Nutzen ist, auch für solche Bereiche, für die keine gesetzliche Verpflichtung besteht, einen Datenschutzbeauftragten zu bestellen oder eine zentrale Datenschutzstelle einzurichten. In einer Reihe von Verwaltungen ist dies auf Empfehlung der DSK bereits geschehen.

Als Voraussetzungen einer wirksamen Aufgabenerfüllung des Datenschutzbeauftragten oder von Mitarbeitern einer zentralen Datenschutzstelle sind zu nennen:

- ausgewiesene Sachkunde,
- unmittelbare organisatorische und fachliche Zuordnung zur Leitung der Dienststelle,
- Verpflichtung aller Verwaltungsbereiche, die Beratung in Fragen des technischen und organisatorischen Datenschutzes in Anspruch zu nehmen.

Es sollten folgende Aufgaben zugewiesen werden:

- Bearbeitung von Grundsatzfragen des Datenschutzes,
- Koordination und Kontrolle von Maßnahmen des Datenschutzes,
- Beratung und Betreuung bei Projekten der technikunterstützten Informationsverarbeitung,
- Beteiligung bei der Vergabe von Zugriffsberechtigungen,
- Information und Fortbildung der Bediensteten in Datenschutzangelegenheiten,
- Federführung beim Schriftverkehr mit dem LfD,
- Kontrolle der Anmeldungen und Änderungsmeldungen zum Datenschutzregister.

20.6.2 Anmeldungen zum Datenschutzregister

Es ist immer wieder festzustellen, daß die Anmeldungen zum Datenschutzregister nicht oder nicht in der durch Gesetz und Verwaltungsvorschrift bestimmten Frist erfolgen. Das Anmeldeverfahren wurde im Berichtszeitraum für zentrale Anwendungsentwicklungen weiter vereinfacht und der mit der Anmeldung verbundene Zeit- und Arbeitsaufwand damit auf ein Minimum reduziert.

20.6.3 Online-Zugriffe auf das Melderegister

In einer größeren Stadtverwaltung verfügten das für EDV-Entwicklungen zuständige Sachgebiet und die Bußgeldstelle über Online-Anschlüsse an das Melderegister und umfassende Abrufmöglichkeiten. Die Online-Übermittlung von Meldedaten war in den genannten Fällen nach den gesetzlichen Bestimmungen nicht zulässig und zur Aufgabenerfüllung nicht erforderlich. Sie wurde aufgrund der Prüfungsfeststellungen eingestellt.

20.6.4 Mitteilungen über Gewerbeanmeldungen

Bei einer Stadtverwaltung wurde festgestellt, daß eine Aufstellung der angemeldeten sowie um- und abgemeldeten Gewerbebetriebe mit dem Datum der Meldung, dem Familiennamen, Vornamen, Geburtsdatum, Geburtsort, Wohnadresse, Betriebsart und -bezeichnung, Betriebsadresse und Datum der Betriebsaufnahme monatlich an 11 Behörden außerhalb der Stadtverwaltung und weitere 13 innerstädtische Ämter weitergegeben wurde. Als Rechtsgrundlage für die Übersendung der Listen wurde eine Regierungsentschließung vom 27. Mai 1953 genannt. Die Überprüfung unter dem Gesichtspunkt der Erforderlichkeit führte zur Reduzierung der Listenübermittlung auf fünf Ämter. Alle weiteren Stellen erhalten nur noch anonymisierte Daten (zu Rechtsfragen im Zusammenhang mit der automatisierten Führung des Gewerberegisters s. oben Tz. 14.2).

20.6.5 Löschung von Daten

Eine Kreisverwaltung hatte bezüglich der Löschung von Daten folgendes verfügt:

- bei Daten von Widerspruchsführern und von sonstigen Beteiligten an einem Widerspruchsverfahren (Löschung nach 30 Jahren),

- bei personenbezogenen Daten von Aussiedlern (keine Löschung),

- bei personenbezogenen Daten von Asylbewerbern (Löschung fünf Jahre nach Wegzug oder Ausweisung).

Die Kreisverwaltung wurde aufgefordert, angemessene Löschungsfristen zu bestimmen. Die sofortige Löschung der Adreßdaten von Personen, die Anträge auf Übernahme Angehöriger in das Bundesgebiet stellten, war geboten, weil die Aufgabe inzwischen von einer Bundesbehörde wahrgenommen wird und die weitere Speicherung bei der Kreisverwaltung nicht mehr erforderlich ist.

20.6.6 AUTISTA-Automation im Standesamt

Die Prüfung der zentralen Verfahrensentwicklung AUTISTA in einer Gemeindeverwaltung ergab, daß beim Starten des PC die in das Verfahren implementierte Paßwortsicherung automatisch umgangen wird. Damit wurde gegen die gesetzliche Verpflichtung verstoßen, angemessene technische Datenschutzvorkehrungen zu treffen.

20.6.7 Wählerverzeichnis der Landtagswahl 1991

Auf der Festplatte eines in einem Standesamt verwendeten Arbeitsplatzrechners waren noch das Wahlprogramm ISIS sowie das Wählerverzeichnis der Landtagswahl 1991 gespeichert.

Die Verwaltung wurde aufgefordert, entsprechend der Verpflichtung nach § 93 Abs. 1 Landeswahlordnung die Daten des Wählerverzeichnisses unverzüglich zu löschen.

20.6.8 PROSOZ-Programmierte Sozialhilfe

Die Dienstanweisung einer überprüften Verwaltung regelte Datensicherungsvorkehrungen, wie sie im Gutachten „Technisch-organisatorischer und persönlicher Datenschutz beim Einsatz von PROSOZ, Hagen 1987" vorgeschlagen werden. Die örtlichen Feststellungen ergaben, daß die getroffenen Festlegungen über den Standort des Fileservers und die Zugangsmöglichkeiten für die z. Z. vorgenommene Installationen der Geräte im Büro des Sozialamtes nicht einzuhalten sind. Nach der Dienstanweisung sollte die Installation in einem EDV-Raum, der einer besonderen Zugangskontrolle unterliegt, erfolgen. Die Festlegungen, daß Sachbearbeiter im Rahmen ihrer Aufgabenerfüllung nur Zugriff auf die Anwendungsprogramme haben und nur Fachvorgesetzte sowie Systemverwalter auf Anwendungsprogramme und zum Betriebssystem, waren nicht realisiert. Jeder Benutzer, der den Fileserver startete, konnte auf das Betriebssystem zugreifen und hatte somit auch die Möglichkeit zur physischen und logischen Datenmanipulation (z. B. Löschen, Kopieren, Verändern und Erstellen von Dateien). Mit dem Ziel, eine wirksame Zugangssicherung zu realisieren, forderte die DSK die Installation des Servers in einem EDV-Raum, der einer besonderen Zugangskontrolle unterliegt. Sie hielt es ferner für geboten, die Zugriffs- und Benutzerkontrolle im Hinblick auf die besondere Schutzwürdigkeit von Sozialdaten durch den Einsatz einer speziellen PC-Sicherungssoftware und -hardware zu verbessern.

20.6.9 Dienstanweisungen für den Datenschutz und die Datensicherheit

Gelegentlich örtlicher Feststellungen, in Beratungsgesprächen sowie bei Anmeldungen zum Datenschutzregister wurde häufig festgestellt, daß bestehende Dienstanweisungen nicht dem veränderten Einsatz von Datenverarbeitungstechnik angepaßt wurden.
Wiederholt wurden auch Kopien der Musterdienstanweisung, die der Orientierungshilfe zu datenschutzrechtlichen Sicherungsmaßnahmen angefügt ist, ohne die erforderlichen Anpassungen an die Bedingungen der datenverarbeitenden Stelle vorgelegt.

Den Empfehlungen der DSK und des LfD, generelle Regelungen über den technischen und organisatorischen Datenschutz in einer allgemeinen Dienstanweisung zu treffen und den Datenschutz beim Einsatz von PC und einem zentralen Rechenzentrumsbetrieb in speziellen Dienstanweisungen bzw. in besonderen Abschnitten zu regeln, wurde entsprochen.

20.7 Anmeldungen zum Datenschutzregister, hier: Textverarbeitungssysteme

In mehreren Beiträgen dieses Tätigkeitsberichts sind Fragen behandelt, die die Führung des Datenschutzregisters betreffen: Für das Verhältnis der richterlichen Unabhängigkeit zur datenschutzgesetzlichen Anmeldepflicht vgl. oben Tz. 7.1.2.1, für die Anmeldepflicht von Wählerverzeichnissen s. u. Tz. 21.6.1.

Wiederholt wurde angefragt, unter welchen Voraussetzungen solche automatisierten Datenverarbeitungssysteme zum Datenschutzregister angemeldet werden müssen, die ausschließlich der Textverarbeitung (Erstellung und Speicherung der dienstlich anfallenden Korrespondenz) dienen.

Vor wenigen Jahren noch konnte hier eine Einschränkung wirksam werden, die auf die technischen Möglichkeiten der eingesetzten Systeme abstellte. Danach waren reine Textverarbeitungssysteme, die keine textübergreifenden Datenauswertungen zuließen, gem. § 10 LDatG nicht anmeldepflichtig, weil aufgrund der Zielsetzung des LDatG nur diejenigen Datenverarbeitungssysteme der Datenschutzkontrolle des LfD bzw. der DSK unterworfen sein sollten, die eine erleichterte Umordnung und Auswertung im Sinne der Dateiverarbeitung ermöglichten.

Im Zuge der technischen Entwicklung sind spezialisierte Textverarbeitungssysteme, die andere Formen der Datenverarbeitung und Datenauswertung (beispielsweise das Speichern und Nutzen von Datenbanken) aus Gründen der technischen

Beschränkung nicht zulassen, kaum noch im Einsatz. Textverarbeitung erfolgt heute regelmäßig auf multifunktional einsetzbaren Geräten, die zwar eine spezialisierte Softwarekomponente „Textverarbeitung" besitzen, die jedoch grundsätzlich die Nutzung des gesamten Instrumentariums der automatisierten Datenverarbeitung (insbesondere der Datenbankerstellung und -nutzung, aber auch der Indexierung von Texten und/oder der umfassenden textübergreifenden Recherchen) zulassen. Wenn die technischen Möglichkeiten zu textübergreifenden Auswertungen vorliegen, ist davon auszugehen, daß eine automatisierte Datenverarbeitung im Sinne des LDatG vorliegt und grundsätzlich die Voraussetzung der Anmeldepflicht gem. § 10 LDatG erfüllt ist.

Als nicht anmeldepflichtig sind dann nur noch solche Verfahren anzusehen, bei denen erstellte Texte, die personenbezogene Angaben enthalten, kurzfristig nach dem Ausdruck gelöscht werden.

Der LfD verkennt nicht, daß damit das Datenschutzregister eine große Zahl von Anmeldungen zu bewältigen hat und daß die Verwaltungen dementsprechend auch mit Anmeldepflichten belastet werden. Andererseits hat er – in Fortsetzung der Bemühungen der DSK – stets Wert darauf gelegt, den technischen Anmeldevorgang so rationell wie möglich zu gestalten und damit die Belastung der Verwaltung gering zu halten. Das Datenschutzregister selbst wird auf einem PC geführt, die personelle Ausstattung der entsprechenden Funktion ist seit Jahren unverändert (eine Halbtagskraft) und wird auch künftig in absehbarer Zeit nicht zu erweitern sein. Der Nutzen dieser Registerführung ist nicht zu unterschätzen: Häufig sind datenschutzrechtliche Defizite (etwa was Löschungen oder Speicherungen nicht erforderlicher personenbezogener Merkmale in automatisierten Systemen betrifft) nur aufgrund von Anmeldungen zum Datenschutzregister bekannt geworden. Erst durch dieses Instrument also kann vorbeugender Datenschutz auch möglichst flächendeckend betrieben werden.

21 Sonstige Tätigkeitsbereiche

21.1 Offenbarung von Eigentumsverhältnissen in einer Rechtsverordnung

Ein Waldbesitzer, der in der Beschreibung der Kernzone eines Naturparks in einer Landesverordnung namentlich benannt worden war, fühlte sich durch diese Namensnennung beschwert. In seiner Eingabe an den LfD argumentierte er, daß er der Beschreibung des Grenzverlaufs unter Nennung seines Namens niemals zugestimmt hätte, denn die Namensnennung offenbare für jedermann die Besitzverhältnisse an einem bestimmten Waldstück.

Das Anliegen des Waldbesitzers ist durchaus berechtigt. Als datenschutzrechtlicher Anknüpfungspunkt mag die Überlegung dienen, daß Auskünfte über die Eigentumsverhältnisse an Grundstücken sowohl aus dem Grundbuch wie auch aus dem Liegenschaftskataster grundsätzlich nur beim Vorliegen eines berechtigten Interesses erteilt werden, eine Bekanntgabe der Eigentumsverhältnisse im Gesetz- und Verordnungsblatt aber diese Zugangsschwelle zu Grundstücksinformationen übergeht.

An das zuständige Ressort ist die Empfehlung zu richten, bei Grenzverlaufsbeschreibungen im Gesetz- und Verordnungsblatt die schutzwürdigen Belange der Grundstückseigentümer zu beachten.

21.2 Umfang des Akteneinsichtsrechts

Einem Antragsteller war der Vertriebenenausweis u. a. deshalb verweigert worden, weil ein ihm unbekannter Zeuge – dessen Anschrift die zuständige Behörde in Erfahrung gebracht hatte – auf Befragung gegenüber dieser Behörde erklärte, daß sich die Großeltern des Betroffenen vor dem Kriege nicht zum deutschen Volkstum bekannt hatten (§ 6 BVFG). Der den Antragsteller vertretende Rechtsanwalt wollte durch Akteneinsicht den Namen und die Anschrift des Zeugen in Erfahrung bringen; die zuständige Behörde hielt die Offenbarung für unzulässig, bat aber um Beratung durch die DSK in dieser Rechtsfrage.

Diese wies darauf hin, daß die Behörde einem Beteiligten nach § 29 Abs. 1 Verwaltungsverfahrensgesetz grundsätzlich Einsicht in die das Verwaltungsverfahren betreffenden Akten zu gestatten hat, soweit die Kenntnis des Akteninhalts zur Geltendmachung oder Verteidigung rechtlicher Interessen erforderlich ist. Vom Vorliegen dieser Voraussetzung war auszugehen.

Die Behörde ist indessen zur Gestattung der Akteneinsicht u. a. dann nicht verpflichtet (§ 29 Abs. 2), soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder dritter Personen, geheimgehalten werden müssen.

Da eine spezielle gesetzliche Regelung nicht existiert, stellte sich die Frage, ob ein mögliches Interesse des Zeugen, gegenüber den Beteiligten an dem Verwaltungsverfahren ungenannt zu bleiben, als berechtigtes Interesse im Sinne dieser Vorschrift anerkannt werden kann.

Die DSK vertrat die Auffassung, daß dies grundsätzlich nicht möglich ist. Zeugen genießen einen so weitgehenden Schutz weder im strafprozessualen noch im zivilprozessualen Verfahren, obwohl dort im Grundsatz eine gesetzliche Zeugnispflicht besteht,

also von Gesetzes wegen – ohne Zustimmung der Betroffenen – in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Die das prozessuale Verfahren bestimmenden Grundsätze, nach denen den Beteiligten eine Prüfung der Beweismittel möglich sein muß, sind auf das Verwaltungsverfahren übertragbar, obwohl oder gerade weil eine Zeugenaussage freiwillig ist. Der Zeuge kann danach nicht erwarten, von einer Überprüfung der Richtigkeit seiner Aussagen durch Beteiligte freigestellt zu bleiben. Eine solche Erwartung wäre jedenfalls nicht „berechtigt" im Sinne des Gesetzes, denn die Zeugenaussage ist als Beweismittel in aller Regel von so großem Gewicht, daß eine Überprüfung des Beweiswertes grundsätzlich möglich sein muß.

21.3 Vollzug des Waffengesetzes

Nummer 32.2.2 der Allgemeinen Verwaltungsvorschrift zum Waffengesetz läßt zu, daß das Bedürfnis für den Erwerb einer weiteren Kurzwaffe bei Sportschützen im allgemeinen anerkannt werden kann, wenn der Antragsteller durch Vorlage einer Bescheinigung des zuständigen regionalen Verbandes nachweist, daß er sich in einer schießsportlichen Vereinigung erfolgreich in bestimmten Schießdisziplinen beteiligt und daß die beantragte Sportwaffe zur Leistungssteigerung erforderlich ist.

Der DSK wurde bekannt, daß einzelne Erlaubnisbehörden sich unmittelbar mit den schießsportlichen Vereinigungen in Verbindung setzten, deren Stellungnahme nach den obigen Bestimmungen einholten und dabei personenbezogene Daten des Antragstellers übermittelten. Dies ist nicht zulässig, da es an einer gesetzlichen Übermittlungsregelung fehlt. Die Verwaltungsvorschrift geht davon aus, daß der Antragsteller jeweils die entsprechende Bescheinigung selbst vorlegt. Es ist nicht vorgesehen, daß die Erlaubnisbehörde sich unmittelbar mit der schießsportlichen Vereinigung in Verbindung setzt. Weigert sich der Antragsteller, die erforderliche Bescheinigung beizubringen, so ist bereits aus diesem Grunde sein Antrag abzulehnen.

Auf Empfehlung der DSK wies das Ministerium des Innern die zuständigen Behörden durch Runderlaß auf die Rechtslage hin.

21.4 Stellung des Geheimschutzbeauftragten einer Behörde

Feststellungen des LfD ergaben, daß der Geheimschutzbeauftragte einer obersten Landesbehörde gleichzeitig Aufgaben als Referent bei der Verfassungsschutzbehörde des Landes wahrnimmt. Diese Praxis, die in organisatorischer Hinsicht zweifelsohne Vorteile haben mag, ist jedoch aus der Sicht des Datenschutzes nicht frei von Bedenken. Die „Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes – Sicherheitsrichtlinien – vom 14. Februar 1989 (MinBl. S. 167) sehen bei der Durchführung der Sicherheitsüberprüfung zunächst die Verfahrensherrschaft des Geheimschutzbeauftragten der jeweiligen Behörde vor und daneben die Mitwirkung des Verfassungsschutzes nach Maßgabe des Landesverfassungsschutzgesetzes und der Richtlinien (s. Ziff. 3.1.1). Ausdrücklich heißt es dort, daß der Verfassungsschutz seine Aufgaben „unbeschadet der Befugnisse des Geheimschutzbeauftragten" wahrnimmt. In dieser Wahrnehmung verschiedener Funktionen durch zwei verschiedene Stellen ist eine bewußte Trennung als rechtsstaatliches Korrektiv auch im Sinne einer Verwirklichung des Rechts auf informationelle Selbstbestimmung zu sehen. Das Ministerium des Innern wurde über diese Auffassung unterrichtet.

21.5 Datenverarbeitung durch private Sicherheits- und Überwachungsdienste

Die Zunahme der Tätigkeit privater Dienste zur Sicherheit und und Bewachung von Personen und Objekten ist zwangsläufig mit dem Erheben und mit der Speicherung personenbezogener Daten verbunden. Der Bayerische LfD hat bereits in seinem 11. Tätigkeitsbericht 1989 über die Möglichkeit berichtet, daß eine Datei errichtet wird, in der „Aktivitäten von potentiellen Tätern" im Umfeld von zu schützenden Personen und Objekten gespeichert werden. Sollte es zu einer überregionalen oder gar bundesweiten Ausdehnung derartiger Dateien kommen, entstünde – soweit sie überhaupt zulässig sind, die Gefahr, daß der in den vergangenen Jahren bei den Polizeibehörden bundesweit erreichte Standard des Datenschutzes unterlaufen wird. In solchen Dateien könnten ähnlich sensible Daten auch von völlig unbeteiligten Bürgern gespeichert werden, wie in den Dateien der staatlichen Sicherheitsbehörden, ohne daß eine Kontrolle durch die unabhängigen Landesdatenschutzbeauftragten möglich ist.

Verstöße gegen Datenschutzbestimmungen können zur Annahme der Unzuverlässigkeit von Gewerbetreibenden führen, sind aber durch die Gewerbeaufsichtsbehörden nicht nachprüfbar. Die Überprüfung der Rechtmäßigkeit von Datenspeicherungen dient nicht gewerberechtlichen Zwecken und fällt daher in den Zuständigkeit der Datenschutzaufsichtsbehörden nach dem BDSG. Um die Nachprüfbarkeit der Rechtmäßigkeit von Datenspeicherungen durch private Sicherungs- und Überwachungsdienste zu erleichtern, sollte wenigstens bis zum Erlaß einer gesetzlichen Regelung angestrebt werden, daß bei der Speicherung personenbezogener Daten in diesem Bereich die jeweilige Datenquelle ausreichend dokumentiert wird.

21.6 Wahlen

21.6.1 Anmeldung zum Datenschutzregister

Im Berichtszeitraum fanden Bundestags- und Landtagswahlen statt. Für diese Wahlen wurde – wie auch für die vorangegangene

Europawahl und die Kommunalwahl – durch Änderung der Wahlordnungen zugelassen, die Wählerverzeichnisse und die Wahlscheinverzeichnisse in automatisierten Verfahren zu führen.

Nach § 10 LDatG besteht für jede Verwaltung im Grundsatz die Verpflichtung, die Anwendung automatisierter Verfahren zur Unterstützung der Wahlvorbereitungen unter Verwendung eines mehrseitigen Vordruckes zum Datenschutzregister anzumelden.

Um den mit Anmeldungen zum Datenschutzregister verbundenen Verwaltungsaufwand zu reduzieren, wurde eine Musteranmeldung ausgearbeitet und in den Verbandsmitteilungen des Gemeinde- und Städtebundes veröffentlicht. Zugleich wurde darauf hingewiesen, daß der Anmeldepflicht nach § 10 LDatG entsprochen ist, wenn in einer formlosen Mitteilung auf diese Musteranmeldung Bezug genommen sowie die im einzelnen angewendeten Verfahren und die Geräteausstattung mitgeteilt werden.

Das verkürzte Anmeldeverfahren hat sich bewährt. Es wurde inzwischen auf zentrale Verfahrensentwicklungen in anderen Verwaltungsbereichen ausgedehnt.

21.6.2 Technische und organisatorische Datenschutzanforderungen bei der automatisierten Führung von Wählerverzeichnissen

Örtliche Feststellungen im Vorfeld der Bundestagswahl ergaben, daß einzelne Wahlämter nicht in der Lage waren, notwendige Änderungen des Wählerverzeichnisses durch Vorlage der Belege nachzuweisen, weil die den Änderungen zugrundeliegenden Mitteilungen der Meldebehörden urschriftlich an diese zurückgegeben worden waren. Die DSK forderte deshalb, daß Mitteilungen, die zu Änderungen des Wählerverzeichnisses führen, zu Nachweis- und Prüfzwecken im Wahlamt verbleiben müssen. Außerdem wurden die Behörden auf Veranlassung der DSK darauf hingewiesen, daß Kopien des Wählerverzeichnisses nur für Sicherungszwecke – und nicht etwa zum Zwecke der Weitergabe an politische Parteien für Wahlwerbezwecke – hergestellt werden dürfen.

Eine Protokollierung von Änderungen des Wählerverzeichnisses und des Wahlscheinverzeichnisses ist im Grundsatz bei allen zur Anwendung kommenden Programmen realisiert. Die nähere Befassung mit einem von einer Vielzahl von Gemeinden praktizierten Verfahren ergab indessen, daß die Protokolldatei vor unzulässigen Eingriffen nicht ausreichend geschützt war. Grundkenntnisse des Betriebssystems DOS und der Datenbanksoftware, die für die Programmerstellung genutzt wurde, reichten aus, beispielsweise das Wählerverzeichnis wie auch die Protokolldatei in der Weise zu manipulieren, daß temporäre Datensätze hinzugefügt und – ohne daß dies nachträglich erkennbar war – wieder entfernt werden konnten. Es war ferner möglich, ohne Protokollnachweis Briefwahlunterlagen mehrfach zu erstellen.

Die DSK hat diese Feststellungen dem Landeswahlleiter mitgeteilt. Bezüglich der Notwendigkeit, zur Vorbereitung von Wahlen nur weitestgehend manipulationsresistente Programme einzusetzen, besteht zwischen allen Beteiligten völlige Übereinstimmung.

22 Schlußbemerkung

Wie in dem Bericht darzustellen versucht wurde, hat der Datenschutz in der abgelaufenen Berichtsperiode bundesweit, aber auch in Rheinland-Pfalz unbestreitbare Erfolge erzielen können und damit sichtbare Verbesserungen in der Rechtsposition der Bürger erreicht. Ganz überwiegend geht dies für Rheinland-Pfalz auf das zielgerichtete Wirken und die Einflußmöglichkeiten der DSK zurück. Sie war stets bestrebt, durch „Datenschutz mit Augenmaß" einen vernünftigen Ausgleich zwischen dem Persönlichkeitsschutz des Bürgers und den Allgemeininteressen der Verwaltung herbeizuführen. Im Verhältnis zu den Behörden wurde demgemäß datenschutzrechtliche Hilfe angeboten und geleistet und, falls notwendig, – auf den Datenschutz bezogen – Kritik geäußert, niemals aber eine Behörde bloßgestellt. Die persönliche Leistung des Kommissionsvorsitzenden, des Abg. Franz Josef Bischel, sowie seines Vertreters, des Abg. Dieter Muscheid und des Kommissionsmitgliedes Abg. Professor Reisinger soll hier mit Dank und Anerkennung erwähnt werden. Besonders hervorzuheben ist die richtungsweisende, koordinierende Tätigkeit des Geschäftsführenden Mitgliedes, Direktor beim Landtag Walter P. Becker, der dies mit der Leitung der Geschäftsstelle leistete; auf ihn ist im wesentlichen die Einführung des Datenschutzes in Rheinland-Pfalz als zweitem Bundesland und viele Jahre vor dem Bund zurückzuführen, so daß er mit Recht zu den Pionieren des Datenschutzes in Deutschland gezählt werden kann.

Was im Lande und im Bund erreicht wurde, geht aber auch auf die enge und loyale Zusammenarbeit mit den Kolleginnen und Kollegen in den anderen Ländern und im Bund sowie mit ihren Mitarbeitern zurück. Ohne den ständigen und intensiven Austausch von praktischen Erfahrungen und Erkenntnissen, ohne bisweilen arbeitsteiliges Vorgehen und insbesondere ohne das gemeinsame Erarbeiten und Durchsetzen von Zielen wäre ein Fortschritt des Datenschutzes heute nur schwer vorstellbar. Dies gilt auch für die seit langem bewährte regelmäßige und enge Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten. Die Reihe der gemeinsamen Aussprachen mit Professor Dr. Simitis und seinen Mitarbeitern soll auch mit dessen Nachfolger, Professor Dr. Hassemer, fortgesetzt werden. Gerade in der Anfangsphase, in der beide Länder als einzige über Kontrollinstanzen des Datenschutzes verfügten, war diese Zusammenarbeit für den damaligen Ausschuß für Datenschutz besonders wertvoll.

Nicht unerwähnt bleiben soll die gute Zusammenarbeit mit der Landtagsverwaltung, der für die tatkräftige Unterstützung der Arbeit des Datenschutzes zu danken ist.

Bei allem, was in den vergangenen Jahren erreicht worden ist, darf jetzt nicht in den Anstrengungen nachgelassen werden, den Datenschutz als freiheitssicherndes Recht für den Bürger gegen die inzwischen auch im politischen Raum stärker gewordenen Widerstände auf seinem jetzigen Stand zu erhalten und weiter auszubauen.

Chancen und Bedrohungen zeichnen sich gleichermaßen ab. Die Art und Weise, in der das Widerspruchsrecht u. a. der öffentlich Bediensteten gegen Aktenüberprüfungen bei Datenschutzkontrollen entgegen der grundgesetzlichen Kompetenzverteilung auch auf die Länder ausgedehnt wurde und wie es teilweise in der Praxis gehandhabt werden soll, zeigt, daß es bundesweit nach wie vor Widerstände aus den verschiedensten Motiven heraus gibt. So sind auch die nach jedem schweren Gewaltverbrechen stereotyp auftretenden Beschuldigungen des Datenschutzes als „Täterschutz" zu werten, bei denen regelmäßig weder ein Beweis noch eine sachlich fundierte oder auch nur plausible Begründung geliefert wird.

Chancen und Zukunftsaufgaben des Datenschutzes liegen in den vielen Bereichen, in denen eine spezifische Ausgestaltung geboten ist. Hier sind beispielhaft der Arbeitnehmerdatenschutz, die datenschutzrechtliche Bewertung der Gentechnologie, der Schutz des informationellen Selbstbestimmungsrechts der Bürger im Justizbereich, insbesondere beim Strafverfahren, und eine datenschutzgerechte Ausgestaltung des Bankgeheimnisses zu nennen. Entscheidende Bedeutung gewinnt der Datenschutz beim Zusammenwachsen Europas, insbesondere in der EG und in deren Mitgliedstaaten.

Hier liegen erhebliche Chancen für eine umfassende Verwirklichung des Persönlichkeitsschutzes in einem „Europa der Bürger". Dort sind aber auch die Gefahren zu suchen, die aus Unkenntnis und Gleichgültigkeit, aber auch aus dem Einfluß materiell interessierter Gruppen kommen. Sie lassen sich schon heute am Beispiel der Behandlung datenschutzrechtlicher Fragen im Zusammenhang mit dem sog. direct-marketing unschwer erkennen.

Der Datenschutz als Dienst für die Rechte der Bürger ist mehr denn je gefordert.

Anlage 1

Entschließung

der 42. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 26./27. September 1991
zum
Datenschutz im Recht des öffentlichen Dienstes

I.

Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß um so konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.

In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z. B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.

Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. Bewerbung um Einstellung in den öffentlichen Dienst

   Es ist – für den Bewerber transparent – festzulegen,

   Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. September 1985, 18. April 1986 und 22. März 1090 nimmt die Konferenz Bezug.

   - welche personenbezogenen Informationen vom ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,

   - ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,

   - ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,

- daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. Sicherheitsüberprüfung

Es ist bereichsspezifisch gesetzlich festzulegen,

- wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
- welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
- wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
- daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
- daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.*)

3. Ärztliche Untersuchung

Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,

- unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
- daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
- wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,
- wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
- daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
- daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecken dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
- daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und – soweit erforderlich – nur tätigkeitsbezogene Risiken mitzuteilen hat,
- daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. Beihilfen

Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. Personalinformationssysteme

Es muß dienstrechtlich gewährleistet sein, daß

- automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z. B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,

---

*) Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. September 1985, 18. April 1986 und 22. März 1990 nimmt die Konferenz Bezug.

- alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,

- Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

Anlage 2

Beschluß

der 40. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
zur Erarbeitung von Krebsregistergesetzen
in Bund oder Ländern
am 4./5. Oktober 1990 in Kiel

1. Die Datenschutzbeauftragten haben schon in ihren Entschließungen vom 14. Dez. 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag der Datenschutzbeauftragten darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.

2. Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Art. 1 i. V. m. Art. 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-/Patientenverhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

   Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt. Sie sind nach wie vor der Meinung, daß Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden können. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sie in Erwägung zu ziehen.

Anlage 3

Beschluß

**der 40. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
zur Stärkung des Schutzes
des Brief-, Post- und Fernmeldegeheimnisses
sowie des nichtöffentlich gesprochenen Wortes
am 4./5. Oktober 1990 in Kiel**

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

- Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wielange telefoniert hat.

- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z. B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.

- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z. B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

- die gesetzlichen Regelungen präziser und enger zu fassen,

- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,

- erlaubte Eingriffe in das Grundrecht nach Art. 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,

- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z. B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereichs gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

Anlage 4

Entschließung

der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 1990 – gegen die Stimme Bayerns – zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungen der Organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz Verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauschgifthandels und sonstiger organisierter Kriminalität – die im übrigen nicht definiert wird –, sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Stafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtliche Bedenken:

- Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung des Gesetzentwurfs in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z. B. auch die Rasterfahndung für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Burger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.

- Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung jeder Straftat – sogar in Wohnungen hinein – „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.

- Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte unverdächtige Personen richten, wenn „aufgrund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.

- Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.

- Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige richterliche Kontrolle zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z. B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

Anlage 5

Entschließung

der 41. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 8. März 1991 zu Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost Telekom (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost Telekom festgehalten werden dürfen, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden – auch Arbeitgeber – auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle – durch die computergesteuerte Vermittlungstechnik entstehenden – Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur

Erstellung des Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen – zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen – müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Artikel 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung – schon aus Gründen der Normenklarheit – in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Anlage 6

Entschließung

**der Sonderkonferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
vom 29. Januar 1991
zum Vorschlag für eine Richtlinie des Rates
zum Schutz von Personen bei der Verarbeitung personenbezogener Daten**

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt diese Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet, die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt – betrachtet man ihre Struktur, Aufgaben und Kompetenzen – diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser – aus den nationalen Datenschutzorganen zusammengesetzten „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 7

Datenschutzrechtliche Anforderungen an den Umgang mit Informationen im Strafvollzugsbereich

1. Datenerhebung

Die Justizvollzugsanstalt erhebt persönliche Daten über den Gefangenen bei diesem selbst, gewinnt eigene Erkenntnisse über den Gefangenen, läßt sich aber auch von Dritten wie anderen Behörden bereits vorliegende Erkenntnisse über den Gefangenen übermitteln. Darüber hinaus findet in der JVA auch eine Datenerhebung über Dritte statt, wobei diese Daten teilweise auch an andere Behörden weitergegeben werden. Ausreichende Rechtsgrundlagen für die Datenerhebung bei Gefangenen über sich selbst oder über Dritte, für die Datenerhebung bei der Polizei oder bei sonstigen Stellen über Gefangene, über Datenerhebungen bei Dritten über Gefangene oder über sich selbst fehlen. Die vorhandenen Rechtsgrundlagen beziehen sich nur auf einzelne Teilbereiche der Datenerhebung, sie sind auch nicht immer genügend präzise (vgl. etwa §§ 5, 6 Strafvollzugsgesetz; 16, 17 VG).

Folgende grundlegende Gesichtspunkte sollten bei künftigen Regelungen berücksichtigt werden: Soweit dies unter den Bedingungen des Strafvollzugs möglich ist, sollten Daten zunächst beim Betroffenen erhoben werden. Werden Daten bei Dritten erhoben, muß darüber nachgedacht werden, wann die betroffenen Personen über Datenspeicherungen zu benachrichtigen, sowie unter welchen Voraussetzungen und wie lange Speicherungen zulässig sind.

Beispielsweise führt die Polizei anläßlich eines Urlaubs des Strafgefangenen eigene Erhebungen durch, wie etwa Erkundigungen bei Nachbarn, Einholung von Bundeszentralregisterauszügen. Soweit die Polizei bislang noch keine Unterlagen über den Gefangenen hatte, wird spätestens jetzt ein Vorgang angelegt. Es ist zu überlegen, ob in derartigen Fällen die Polizei nur auf ihre eigenen, bereits vorhandenen Unterlagen und Kenntnisse zurückgreifen sollte und notwendige Bundeszentralregisterauszüge unmittelbar durch die JVA angefordert werden sollten. Auch in diesem Zusammenhang sollte der Erforderlichkeitsgrundsatz berücksichtigt werden und die Intensität der Datenerhebung abhängig sein beispielsweise von der Dauer der Strafe und der Schwere der Tat.

a) Das Verfahren der Aufnahme (§ 5 Strafvollzugsgesetz, Nr. 16 VGO, VG 3 und 4)

Nr. 16 VGO enthält einige Regelungen zur Aufnahmeverhandlung. Der Verhältnismäßigkeitsgrundsatz ist allerdings zu wenig berücksichtigt. Nur die im jeweiligen Einzelfall erforderlichen Daten sollten erhoben werden. Die Verweildauer des Gefangenen sollte hierbei berücksichtigt werden. Die aktuellen Regelungen stellen zu sehr auf Langstrafen ab. Zu prüfen ist, inwieweit im Vordruck VG 3 die Vorstrafen im bisher vorgesehenen Umfang aufzuführen sind.

b) Vorstellung beim Anstaltsleiter (Nr. 29 VGO, VG 14)

Das Gespräch zwischen Anstaltsleiter und Gefangenen entzieht sich einer gesetzlichen Regelung. Dem Anstaltsleiter kann die Stellung eines Beichtvaters zukommen. Es darf jedoch kein besonderer Druck ausgeübt werden, um Daten aus dem besonders geschützten Bereich der Privatsphäre (vgl. § 5 Abs. 1 Strafvollzugsgesetz) zu erheben.

Die Verwendung des sogenannten „leeren Bogens" (VG 14), der für die Niederlegung eines Lebenslaufs bestimmt ist, ist insoweit unbedenklich, als Bemerkungen zu Tatsachen, die vollzugsrelevant sind, aufgenommen werden. Feststellungen zu charakterlichen Eigenschaften in diesem frühen Stadium des Vollzugs (wie verstockt, offen etc.) sollten jedoch nur im unabdingbar erforderlichen Umfang erfolgen. Der Vermerk des Anstaltsleiters über das Ergebnis der Vorstellung vermittelt den Einstieg für die weitere Behandlung, ihm kann daher entscheidende Bedeutung für den weiteren Verlauf des Vollzugs zukommen. Die Feststellung der personenbezogenen Daten muß daher äußerst sorgfältig erfolgen. Sensible Daten, denen keine aktuelle Bedeutung zukommt, sollten außerhalb der eigentlichen Vollzugsakten, z. B. in einem Sonderheft, festgehalten werden, falls sie für erforderlich erachtet werden.

c) Ärztliche Untersuchung (§ 5 Abs. 3 Strafvollzugsgesetz, Nr. 60 VGO, VG 13)

Die Datenerhebung durch den Anstaltsarzt kann nicht beschränkt werden, soweit es sich um medizinisch relevante Umstände handelt, über deren Erhebung der Arzt grundsätzlich selbst zu entscheiden hat. Eine Regelung der Datenerhebung (und der Datenübermittlung) könnte auf §§ 56, 101 Strafvollzugsgesetz aufbauen. Allerdings müßte deutlicher geregelt werden, daß jeder Gefangene ärztlich zu untersuchen ist und welche Maßnahmen hierbei zulässig sind.

Eine (freiwillige) Preisgabe oder Offenbarung von Daten an die Justizvollzugsanstalt kann bereits in der Aufnahmeverhandlung stattfinden. Soweit diese Informationen auf dem A-Bogen aufgenommen werden, würden sie unter anderem

jedoch auch in die Kleiderkammer gelangen. Dies sollte unterbunden werden, damit die bereits praktizierte Trennung zwischen Personal- und Gesundheitsakten nicht unterlaufen wird. Diese Trennung und die jeweils unterschiedliche Berechtigung für den Zugriff sollten in den Vorschriften (vgl. auch Nr. 60 VGO) deutlicher zum Ausdruck kommen.

d) Erkennungsdienstliche Maßnahmen (§ 86 Strafvollzugsgesetz, vgl. auch Nr. 23 VGO und VG 9)

Es muß geprüft werden, ob Personen, die eine Ersatzfreiheits oder Kurzstrafe verbüßen, erkennungsdienstlich behandelt werden müssen. Die insoweit erhobenen Daten dürfen grundsätzlich nur in der JVA gespeichert werden.

Eine Funktionstrennung – wie sie § 81 b StPO vorsieht – sollte vorgenommen werden. Dabei sollte deutlich gemacht werden, ob und welche erkennungsdienstlichen Maßnahmen zur Durchführung des Strafvollzugs oder für Fahndungsmaßnahmen erforderlich und zulässig sind.

e) Behandlungsuntersuchung (§ 6 Strafvollzugsgesetz, Nr. 31 VGO, VG 16 und 17: Lebenslauf und Fragebogen)

Die Behandlungsuntersuchung wirft aus datenschutzrechtlicher Sicht folgende Problemkreise auf:

- Die Behandlungsuntersuchung als Erforschung der Persönlichkeit und der Lebensverhältnisse des Gefangenen stellt eine umfassende Erhebung von personenbezogenen Daten dar. Neben solchen des Gefangenen werden in nicht unerheblichem Umfang auch Daten Dritter (z.B. von Familienangehörigen) bekannt, wovon diese regelmäßig keine Kenntnis erlangen. So wird etwa nach Namen, Alter, Beruf und Wohnort der Geschwister gefragt. Weiterhin wird nach den früheren und jetzigen Verhältnis zu ihnen geforscht. Zwar dürfte es grundsätzlich datenschutzrechtlich unbedenklich sein, das Verhältnis des Gefangenen zu Geschwistern zu erfassen. Dabei dürfte es jedoch nur in dem für den Vollzug erforderlichen Umfang auch unabdingbar sein, personenbezogene Daten über die Geschwister selbst zu erheben. Eine anonymisierte Datenerhebung sollte Vorrang haben, soweit dies überhaupt möglich ist.

- Mitteilungen, die erkennbar den höchstpersönlichen Lebensbereich betreffen, sollten nur dann in eine Gefangenenkonferenz eingebracht werden, wenn dies unbedingt erforderlich ist. Der Bedienstete der JVA, der zugleich Vertrauensperson und Entscheidungsträger ist, also auch Entscheidungen „gegen" den Gefangenen treffen muß, muß dies im Vorhinein bei Gesprächen mit dem Gefangenen klarstellen.

- Soweit einzelne Daten für einzelne Bedienstete der JVA (z.B. den Psychologen) von Bedeutung sind, sollten nur diese die entsprechenden Informationen erhalten. Wahrnehmungs- und Beurteilungsbögen können durch viele Hände gehen. Bei Psychologen und Sozialarbeitern ergeben sich ähnliche Probleme im Rahmen des § 203 StGB wie bei Ärzten. Führung von Sonderheften und unbedingte Beachtung der Zweckbindung erscheinen auch deshalb dringend geboten.

- Es sollte erwogen werden, bei der Datenerhebung zu unterscheiden zwischen Grunddaten, die für jeden Gefangenen erhoben werden müssen und besonderen Daten, die nur für einzelne Gefangene und nur von bestimmten Bediensteten zu erheben sind. Auch insoweit könnte an den Einsatz eines Sonderheftes gedacht werden.

f) Überwachung des Schriftwechsels (§§ 29 ff. Strafvollzugsgesetz; Nrn. 37 ff. VGO)

Die Überwachung des Schriftwechsels von Untersuchungshäftlingen obliegt dem Richter (Nr. 30 UVollzO). Bei Strafgefangenen hat sie der Anstaltsleiter oder ein von ihm beauftragter Bediensteter zu führen. Es sollte geprüft werden, ob die Überwachung zentral und nicht vom jeweiligen Stationsbeamten durchgeführt werden kann, denn das Briefgeheimnis und eine weitestmöglich freie Kommunikation sollten gewährleistet werden.

Nach § 29 Abs. 2 Strafvollzugsgesetz werden Schreiben des Gefangenen an Volksvertretungen des Bundes und der Länder bei Vorliegen der weiteren dort genannten Voraussetzungen nicht überwacht. Entsprechendes sollte für den Schriftwechsel mit dem Datenschutzbeauftragten gelten.

Die Behandlung angehaltener Schreiben wird bisher in § 31 Abs. 3 Strafvollzugsgesetz und Nr. 39 VGO geregelt; auch diese Schriftstücke sollten in das oben vorgeschlagene Sonderheft aufgenommen werden. Bei der Entlassung sollten diese Schreiben grundsätzlich ausgehändigt oder vernichtet werden, da eine Sicherheitsgefährdung der Anstalt dann regelmäßig nicht mehr vorliegt. Besonders bedeutsam ist eine derartige Handhabung auch für die Ablichtung von Schreiben Dritter an den Gefangenen, wenn sie kopiert und in die Gefangenenakten aufgenommen worden sind.

g) Überprüfung im Zusammenhang mit Vergünstigungen

Bei Überprüfungen im Zusammenhang mit Urlaub, Besuch u. ä. sind häufig Daten Dritter zu bearbeiten. Grundsätzlich

sind diese Daten nur mit Einwilligung aller Betroffenen zu erheben. Vor der Einwilligungserklärung sollten die beabsichtigten Datenerhebungsmaßnahmen bei der Polizei, der Nachbarschaft usw. offengelegt werden.

2. Datenspeicherung

Zur Person jedes Gefangenen führen die Justizvollzugsanstalten Unterlagen in verschiedener Form. Zu untersuchen sind insbesondere zur Person des Gefangenen geführte Akten, die Aufnahme von personenbezogenen Informationen in (bisher überwiegend manuellen) Dateien, die ihre Aufgabe und Zweckbestimmung jeweils durch den mit ihnen verbundenen Sachverhalt erfahren und weitere Aktensammlungen, vorwiegend in Form von Büchern zur chronologischen Dokumentation bestimmter Vorgänge. Die Speichermedien im einzelnen:

a) Zur Person jedes Gefangenen werden Strafvollzugsakten, für die die Aktenordnung nicht gilt, geführt.

aa) Die Gefangenenpersonalakten

Die Gefangenenpersonalakte bildet das Herzstück der personenbezogenen Aktenführung über jeden Insassen einer JVA. Sie findet indirekt ihre Rechtsgrundlage in §§ 5 – 7 Strafvollzugsgesetz, konkretisiert in Nr. 58, 59 VGO, die abgesehen von Ausnahmen die Anlegung einer Personalakte als Regelfall vorsehen. Die Personalakte stellt sich als Sammelakte dar, die eine Vielzahl verschiedener, formalisierter Einzelvorgänge zusammenfaßt. Bereits die äußere Form des Schnellhefters, der diese Einzelunterlage enthält, weist z.B. daraufhin, ob der Gefangene lediglich zu einer Freiheitsstrafe bis zu drei Monaten verurteilt worden ist (VG 47) oder eine längerfristige Freiheitsstrafe zu verbüßen hat (VG 45 bzw. VG 46).

Die in Nr. 59 Abs. 1 VGO im einzelnen dargelegten und in 3 Heftnadeln unterschiedenen Einzelvorgänge verdeutlichen die Komplexilität der erfaßten Informationen:

Die Heftnadel 1 enthält mit einer Personenbeschreibung, den Vermerk über die Vorstellung zum Anstaltsleiter (VG 14), den Lebenslauf (VG 16) und den sogenannten Fragebogen (VG 17) mehr Daten, als eine schnelle Information zu einem Gefangenen erfordert. Hier wird eine Vielzahl auch intimer und die Persönlichkeit des Gefangenen im Kern betreffender Informationen niedergelegt. Bisher gibt es keine differenzierten Regelungen für Speicherung und Verwendungszwecke dieser Unterlagen und der übrigen Bestandteile der Gefangenen-Personalakte. Es wird vorgeschlagen, die Verwendung und folglich den Zugang zu der Akte auch dadurch differenziert zu gestalten, daß durch Anlegen verschiedener Teile der Personalakte und eine Differenzierung der Zugangswege nur die jeweils erforderlichen Teile verwendet werden.

Die Heftnadel 2 der Personalakte enthält jeweils das vollständige Urteil, das auch Daten über eine Vielzahl Betroffener enthalten kann (§ 59 Abs. 2 VGO). Auch dies macht die Erforderlichkeit einer strengen Zweckbindung der in der JVA verarbeiteten Daten deutlich. Die in der zweiten Heftnadel enthaltenen Einweisungsunterlagen enthalten bisher auch die jeweilige Anklageschrift. Außer in den Fällen der Untersuchungshaft könnte darauf im Regelfall wohl verzichtet werden, wenn ein Urteil vorliegt.

Die in Heftnadel 3 zusammengefaßten Schriftstücke enthalten zum Teil ebenfalls sensible Daten wie z.B. Disziplinarmaßnahmen (VG 52) oder angehaltene Schreiben (vgl. Nr. 39 VGO). Solche Unterlagen sollten in einem Sonderheft zusammengefaßt werden, das nur dann zur Verfügung gestellt werden soll, wenn dies auch für die anfordernde Dienststelle erforderlich ist.

bb) Die Gesundheitsakte

Die vom Arzt geführte Gesundheitsakte besteht im wesentlichen aus folgenden Vordrucken: Schnellhefter (VG 53), Personalblatt (VG 3), Gesundheitsblatt (VG 54) und Behandlungsblatt (VG 55). Die hier gespeicherten Daten sind äußerst sensibel. Das derzeitige System, die Akte nur beim Arzt zu führen und von der Personalakte zu trennen, muß beibehalten werden. Die Abschottung verdient hier absolute Priorität. Besonders für diese Akten sind wirksame und klare Verwendungsregelungen zu schaffen. Die Problematik der Herausgabe von Daten muß unter Berücksichtigung von § 203 StGB gelöst werden. Sämtliche Phasen der Datenverwendung müssen gesetzlich vorgegeben werden. Informationen, die auf einem Verdacht beruhen oder die ungesichert sind, müssen als solche gekennzeichnet werden. Dies ist insbesondere bei dem Vermerk „Vorsicht Blutkontakt" zu beachten, soweit nicht eindeutige Untersuchungsergebnisse (etwa zur Ansteckungsgefährdung bei Hepatitis B) vorliegen. Soweit bei einer automatisierten Datenverarbeitung sogenannte Sicherheitsvermerke benutzt werden, die den ärztlichen Bereich betreffen, ist ebenfalls ein gesetzlicher Rahmen vorzugeben.

cc) Weitere Akten, Personalbeiakten

Sonderakten führen etwa auch Pfarrer und Anstaltspsychologen. Diese Akten enthalten anlaßbezogene Unterlagen, die auf der Grundlage von formalisierten Bögen vorgehalten werden. Der Umfang der erhobenen Daten hängt von der Persönlichkeit des betreffenden Amtsträgers ab. Für diese Unterlagen müssen die gleichen Grundsätze gelten wie auch für die Gesundheitsakten. Ebenso muß geklärt werden, inwieweit solche besonderen Betreuungspersonen Zugang zu den übrigen Akten erhalten und inwieweit sie diese verwenden dürfen. Die Informationen sollen in die Vorgangsverwaltung (dritte Heftnadel) übernommen werden, sobald sie für die Arbeit der JVA nicht mehr von Bedeutung sind. Weitere anlaßbezogene oder funktionsbezogene Unterlagen wie etwa Urlaubsgesuche und darauf bezogene Schriftstücke oder Unterlagen im Zusammenhang mit dem Arbeitseinsatz sollen als Personalbeiakten geführt und nur bei Erforderlichkeit im Einzelfall verwendet werden.

b) Dateien

Im Bereich des Strafvollzugs werden eine Vielzahl manueller und zum geringeren Teil auch automatisierte Dateien geführt. Die automatisierte Datenverarbeitung in den JVA wird jedoch stark zunehmen. Rechtsverordnungen oder zumindest Errichtungsanordnungen, die Rahmenbedingungen verbindlich festlegen, gibt es bisher wohl nicht. Anhaltspunkte für die Novellierung können die für das Strafverfahren als regelungsbedürftig anerkannten Bereiche geben (vgl. das StVÄG). Zugriff, Sicherungsmaßnahmen etc. sollen bereichsspezifisch geregelt werden.

Nach dem Kenntnisstand der Datenschutzbeauftragten werden derzeit folgende Dateien geführt:

- Das Gefangenenbuch (K), das gemäß Nr. 66 VGO (vgl. auch VG 58, 59) den Nachweis über anwesende, vorübergehend anwesende und entlassene Gefangene aufweist, wenn es – wie im Regelfall – als Datei geführt wird;

- eine Reihe funktional bedingter Karteien wie die Kleiderkammerkartei, die ein Verzeichnis der eingebrachten Habe, der ausgegebenen Kleidungsstücke und sonstiger Gegenstände enthält;

- die Arbeitskartei mit Informationen über die im jeweiligen Bereich arbeitenden Gefangenen;

- die Abrechnungskartei mit Nachweisen über Arbeitsleistungen und Zahlungen von Arbeitsentgelt;

- Eigengeldkonten;

- die an verschiedenen Stellen der JVA geführten „Wahrnehmungsbogen", die zu einem späteren Zeitpunkt jeweils in die Personalakte eingeführt werden können und die von verschiedenen Stellen ausgefüllt werden wie Abteilungsleiter, Erziehungsgruppenleiter, Geistlichen, Psychologen, Sozialpädagogen, Lehrern, Sozialarbeitern oder zuständigen Bediensteten des allgem. Vollzugsdienstes, des Werksdienstes und eventuell auch des Sicherheitsbereichs. Eine Sammlung solcher Wahrnehmungsbogen stellt eine Datei im datenschutzrechtlichen Sinne dar;

- besonders sensible Informationen enthält die Kartei potentieller Störer in einer „Gefahrenkartei". Justizvollzugsanstalten, deren Verwaltungen EDV-unterstützt arbeiten, speichern zunehmend sogenannte Sicherheitsvermerke (wie Fluchtgefahr, gewalttätig, Freitodgefahr, Trennungsvermerke usw.). Die Vergabe der Vermerke erfordert besondere Sorgfalt, da eine unrichtige Speicherung diskriminierend wirken kann. Die Voraussetzungen für die Aufnahme eines Sicherheitsvermerks, dessen Speicherungsdauer und die Löschungsfristen müssen geregelt werden, wobei im medinzinischen Bereich unter Umständen besondere Sicherungsmaßnahmen veranlaßt sind;

- sensible Daten enthalten auch Karteien der Drogenabhängigen oder die Sammlung von Aufnahmeersuchen bei Nichtantritt von Ersatzfreiheitsstrafen;

- die Besucherkartei (Nr. 36 VGO, VG 22) enthält Daten über solche Personen, die die Gefangenen besuchen. Polizeiliche Erkenntnisse und Bundeszentralregisterauszüge werden in diesem Rahmen erhoben (vgl. unten den Abschnitt Häftlingsüberwachung). Nr. 36 VGO ist hierfür keine ausreichende Rechtsgrundlage.

Die Speicherung von Informationen in derartigen Dateien bedarf normenklarer gesetzlicher Regelungen, durch die die Erhebungs- und Verwendungsbedingungen festgelegt werden. Dazu gehört auch die Verwendung von Daten, die eventuell aus dem Bundeszentralregister, von Polizeidienststellen oder anderen außenstehenden Institutionen stammen. Notwendig sind auch Regelungen über die Weitergabe der in diesen Dateien enthaltenen Daten, etwa an Polizeidienststellen, zum Zwecke der Haftüberwachung oder sonstigen Zwecken Dritter.

Ein weiteres Problem stellt die parallele Führung solcher Karteien nach Namen oder sachlichen Funktionen dar. Eine Parallelführung sollte nur im Ausnahmefall zugelassen werden, wenn sie unabdingbar ist. Die Aktualisierung der Dateien muß in jedem Fall gewährleistet sein.

c) Weitere Datensammlungen

Insbesondere in Form von Büchern oder Listen werden eine Reihe von Informationssammlungen geführt, für die nicht unmittelbar die gleichen Bedingungen gelten können wie für die Personalakten oder Dateien. Dies gilt insbesondere für das Gefangenenbuch (N – VGO Nr. 66 – VG 60 mit Namensverzeichnis), soweit es tatsächlich als Buch geführt wird und nicht als Datei. Gleiches kann übrigens auch für das Gefangenenbuch (K) gelten, soweit es als Buch geführt werden sollte, das Zugangs-Abgangsbuch (VGO Nr. 67 – VG 62, 63), das Belegungsbuch, Frühbericht (VGO Nr. 68 – VG 64, 65), den Abgangskalender (VGO Nr. 69 – VG 66), das Krankenbuch (VGO Nr. 70 – VG 67) sowie sonstiges Buchwerk etwa über Disziplinarmaßnahmen (VG 68), besondere Sicherungsmaßnahmen (VG 69), Beurlaubungen (VG 70), Entweichungen (VG 71), Freigang (VG 72), Ausgang (VG 73) sowie Listen über den Posteingang und Postausgang und eventuell über telefonische Kontakte.

Für diese Werke gilt zwar das für Dateien Gesagte entsprechend. Dabei ist allerdings zu berücksichtigen, daß das Medium Buch bzw. Liste schon aus praktischen Gründen besondere Regelungen erfordert. Dies gilt namentlich bei Löschungen (Problem des Zusammenhangs mit anderen Daten bzw. der fortdauernden Erkennbarkeit ausgestrichener Worte) sowie bei der Übermittlung, die insbesondere bei der Gewährung von Einsichtnahme die Möglichkeit birgt, daß auch überschüssige Informationen zur Kenntnis genommen werden. Aus diesem Grund sind die Verwertungsbedingungen unter Berücksichtigung des Mediums im einzelnen exakt und restriktiv festzulegen.

Zusammengefaßt ist die Schaffung abschließender Regelungen für alle Speichermedien zu fordern, die personenbezogene Daten enthalten. Überflüssige Doppelspeicherungen sind zu vermeiden. Die Richtigkeit der Daten ist zu gewährleisten. Zum Einsichtsrecht für Gefangene siehe unten.

3. Datenübermittlung

a) Datenübermittlung im Gesundheitsbereich

Übermittlungen von Gesundheitsdaten sollten grundsätzlich gesetzlich geregelt werden. Relevante gesundheitsbezogene Tatsachen dürfen im Rahmen des Verwaltungsvollzugs lediglich im jeweiligen Einzelfall weitergegeben werden.

Ein Großteil der AIDS-Hinweise kommt beispielsweise aus Justizvollzugsanstalten. Diese und andere Datenübermittlungen erfolgen insbesondere auch im Zusammenhang mit Verschubungen. Hier ist auf eine streng zweckgebundene Verwendung zu achten: Solange die Verschubung andauert, dürfen die Erkenntnisse verwertet werden. Sie dürfen jedoch grundsätzlich nicht in den allgemeinen polizeilichen Aufgabenbereich übernommen werden.

Daten können faktisch auch dadurch etwa an Mitgefangene übermittelt werden, daß besondere Vollzugsmaßnahmen für einzelne Mitgefangene getroffen werden. Es ist zu verhindern, daß Kranke mehr als notwendig und in einer Weise aus dem Allgemeinvollzug herausgenommen werden, die Rückschlüsse auf die Art der Erkrankung zulassen. Dies betrifft auch etwa die Anbringung von Vermerken für besondere Ernährung auf den Zellentüren oder die Gewährung von Vergünstigungen wegen Krankheit. Eindeutige Rückschlüsse sind nach Möglichkeit auszuschließen. Für Vermerke wie etwa „Vorsicht Blutkontakt!" sollte zumindest eine gesetzliche Rahmenregelung gefunden werden.

Probleme bereitet immer wieder die Zulässigkeit einer Offenbarung von an sich nach § 203 StGB geschützten Daten. Reine Verwaltungsvorschriften können dabei keine rechtfertigende Befugnis zur Offenbarung im Sinne der obengenannten Strafvorschrift geben. Vielmehr muß auch hier eine gesetzliche Regelung erfolgen. § 34 StGB (rechtfertigender Notstand) reicht als Handlungsgrundlage für die Verwaltung grundsätzlich nicht aus.

b) Auskünfte an Private

Nr. 5 Abs. 3 VGO enthält eine Regelung zu Auskünften über Gefangene an private Personen und Stellen. Diese Regelung muß – auch im Hinblick auf die uneinheitliche Rechtsprechung in diesem Zusammenhang – präzisiert werden, insbesondere muß der Umfang der gegebenenfalls zu übermittelnden Daten festgelegt werden. Es sollte hierbei an die melderechtlichen Regelungen über Auskünfte angeknüpft werden, die Insassen von Justizvollzugsanstalten betreffen. In § 25 Abs. 3 Satz 2 Landesmeldegesetz Rheinland-Pfalz ist dazu beispielsweise geregelt, daß die Meldebehörde Informationen über Insassen von Justizvollzugsanstalten nur übermitteln darf, wenn sie durch Prüfung im Einzelfall festgestellt hat, daß durch die Übermittlung keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden. Schutzwürdige Belange

werden insbesondere beeinträchtigt, wenn die Übermittlung gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck den Betroffenen unverhältnismäßig belastet. Vor Melderegisterauskünften hat die Meldebehörde den Insassen der JVA zu hören.

Diese Restriktionen dürfen nicht dadurch umgangen werden, daß ein auskunftbegehrender Dritter sich – statt an die Meldebehörde – unmittelbar an die JVA wendet.

c) Übertragung von Hilfsdiensten an Mitgefangene

In der Praxis werden Gefangene häufig mit der Durchführung von Vollzugsaufgaben betraut. Dabei muß eine Regelung getroffen werden, inwieweit sie im Rahmen ihrer Tätigkeit Kenntnis über Daten von Mitgefangenen erhalten dürfen. Der Umfang der Daten ist auf das unumgänglich Notwendige zu beschränken. Beispiel: Das Aushändigen geöffneter Post durch Mitgefangene sollte unterbleiben.

d) Zusammenarbeit der im Vollzug tätigen öffentlichen Stellen

§ 154 Strafvollzugsgesetz schreibt die Zusammenarbeit der Vollzugsbehörden mit anderen öffentlichen Stellen vor. Gegenwärtig erhalten diese Stellen oftmals mehr Daten über den Gefangenen, als es für die Erfüllung der eigenen Aufgabe erforderlich ist. Da es bei der Betreuung des Gefangenen durch Bewährungshilfe und Führungsaufsicht auch um die Kenntnis der Person des Betroffenen geht, wird die Definition eines Datenkatalogs, der übermittelt werden darf, kaum möglich sein. Zumindest sollte jedoch der Erforderlichkeitsgrundsatz in die Regelung aufgenommen werden.

Da die Tätigkeit der Entlassenenfürsorge, der Sozialhilfe und sonstiger Verbände der freien Wohlfahrtspflege vom entlassenen Gefangenen freiwillig angenommen wird, sollten Daten an diese Stellen auch nur mit seiner Einwilligung übermittelt werden. Bei der Übermittlung an das Arbeitsamt und an die Sozialversicherung ist für die jeweiligen Empfänger nur die Kenntnis bestimmter Daten erforderlich. Diese sollten abschließend aufgezählt werden.

e) Mitteilungen über die Entlassung an andere Behörden

Spiegelbildlich zu den Aufnahmemitteilungen scheint auch die Erforderlichkeit einiger Entlassungsmitteilungen klärungsbedürftig. Dies gilt hinsichtlich § 52 Abs. 2 VGO (Unterrichtung des Jugendamts), § 52 Abs. 3 VGO (Unterrichtung der Erziehungsbehörde). Die Regelung für Mitteilungen an die Erfassungsbehörde, an die Kreiswehrersatzämter und an die Bundeswehr sind lückenhaft: An die Bundeswehr wird die Entlassung eines Bundeswehrangehörigen, nicht jedoch die Aufnahme mitgeteilt (§ 52 Abs. 6 VGO). Wie bei Wehrpflichtigen verfahren wird, ist nicht geregelt.

Um dem Grundsatz der Normenklarheit Rechnung zu tragen, müßten hier gegebenenfalls Ergänzungen vorgenommen werden. Dabei ist zu berücksichtigen, daß die genannten Stellen nur – wenn erforderlich – Kenntnis über einen JVA-Aufenthalt erhalten sollen. Eine pauschale Übermittlung von Daten sämtlicher in Haft befindlicher Personen, die der Wehrüberwachung unterliegen, scheidet damit aus. Sofern der Betroffene unter einem anderen Wohnsitz gemeldet ist, dürfte kein Anlaß für eine Mitteilung bestehen, da er die Unterlagen über diese Adresse erhalten kann.

f) Paketmarken

Die Verpflichtung zur Verwendung von Paketmarken, durch die der Gefangene gezwungen wird, seinen Aufenthaltsort zu offenbaren, ist auf das Notwendige zu beschränken. Es darf nicht für alle möglichen Sendungen die Verwendung von Paketmarken verlangt werden. § 33 Strafvollzugsgesetz sollte die entsprechenden Sachverhalte regeln.

g) Haftraumbeschilderung

Bei der Beschriftung der Haftraumschilder ist auf die Belange des Gefangenen Rücksicht zu nehmen, der grundsätzlich ein Recht darauf hat, das seine persönlichen Daten (insbesondere auch Gesundheitsdaten) nicht Außenstehenden oder Mitgefangenen zur Kenntnis gelangen. Es ist daher ein abschließender Katalog zu erstellen, welche Angaben zulässigerweise auf den Haftraumschildern enthalten sein dürfen.

h) Lohnsteuerkarte

Beantragt ein in der JVA gemeldeter Gefängnisinsasse eine Lohnsteuerkarte, wird als Wohnanschrift die JVA-Adresse eingetragen. Dadurch erlangen Arbeitgeber und Finanzamt Kenntnis vom Aufenthalt in der JVA. Eine Lösung dieses Problems kann darin bestehen, die Gefangenen darauf hinzuweisen, erst nach der Entlassung die Erteilung der Lohnsteuerkarte zu beantragen. Dabei ist dann – unabhängig vom Stichtag des § 39 Abs. 2 EStG – der neue Wohnsitz als Anschrift einzutragen.

i) Akteneinsicht durch Dritte

Die Akteneinsicht ist in Nr. 5 Abs. 4 VGO geregelt. Es sollte klargestellt werden, daß Privatpersonen grundsätzlich keine Einsicht in die Personalakte eines Gefangenen gewährt werden kann. Ausnahmen sind abschließend zu regeln.

4. Auskunftsansprüche und Akteneinsichtsrechte des Strafgefangenen

In Anlehnung an die von der Rechtsprechung dazu entwickelten Grundsätze sollte auch ein gesetzlich begründeter Auskunfts- bzw. Akteneinsichtsanspruch durch Strafgefangene in die sie betreffenden Unterlagen geschaffen werden.

5. Sicherungsmaßnahmen; Löschung personenbezogener Daten Strafgefangener

Im Bereich der Gefangenenverwaltung sind bereichsspezifische Regelungen für die Datenverarbeitung in Akten und Dateien und für die automatisierte Datenverarbeitung erforderlich, die den besonderen Verhältnissen des Strafvollzugs Rechnung tragen. Datensicherungsmaßnahmen sollten das Ziel verfolgen, daß nur ein kleiner Kreis von Berechtigten Zugriff auf die Daten hat und sowenig Personen wie möglich Kenntnis von der Inhaftierung des Betroffenen erhalten.

Um den Resozialisierungsgedanken zu beachten und die Rechte des Gefangenen nicht unnötig zu beeinträchtigen, sind nach seiner Entlassung differenzierte Löschungsvorschriften bezogen auf die anläßlich seiner Inhaftierung gespeicherten Daten im Strafvollzugsgesetz erforderlich. Bei automatisierter Datenverarbeitung ist durch eine Anpassung der Technik den Anforderungen des Datenschutzes Rechnung zu tragen. Die im allgemeinen Datenschutzrecht vorgesehenen technischen und organisatorischen Maßnahmen sind praktisch durchzuführen.

a) Personalakte und Sonderheft

In der Personalakte befindet sich eine Fülle personenbezogener Daten, die nur zum Teil über den Entlassungstermin des Gefangenen hinaus benötigt werden. Die durch einzelne Justizverwaltungsvorschriften vorgesehenen Aufbewahrungszeiträume von 30, z. T. sogar bis zu 50 Jahren erscheinen als erheblich zu lang. Differenzierte Löschungsfristen erscheinen daher angebracht. Grundsätzlich ist darauf zu achten, daß nur solche Informationen länger aufbewahrt werden, die auch nach der Entlassung des Gefangenen benötigt werden. Dies sind im wesentlichen die Personalien des Gefangenen, seine Verweildauer in der Anstalt sowie Informationen über dessen persönliche Entwicklung.

Anknüpfungspunkt für die Aufbewahrungsdauer von Unterlagen könnte möglicherweise die Zeitspanne der Freiheitsstrafe sein, zu der der Gefangene verurteilt worden ist, oder der Zeitraum, den der Gefangene tatsächlich in der Strafanstalt verbracht hat. Bei der Vollstreckung von Ersatzfreiheitsstrafen dürfte der Verhältnismäßigkeitsgrundsatz besonders kurze Löschungsfristen erforderlich machen.

Erkennungsdienstliche Maßnahmen dienen nach § 86 Abs. 1 Strafvollzugsgesetz der Sicherung des Vollzugs. Solche Unterlagen sollten grundsätzlich in der JVA bei der Entlassung des Gefangenen vernichtet werden. Hierfür spricht auch, daß nach Nr. 23 Abs. 3 VGO Lichtbilder in Abständen von drei Jahren zu erneuern sind. Ein Antrag des Gefangenen sollte künftig nicht Voraussetzung der Vernichtung sein.

Hinsichtlich der übrigen Informationen über die persönliche Entwicklung des Gefangenen ist zu prüfen, ob eine Löschung dieser Daten nicht bereits fünf Jahre nach Entlassung des Gefangenen erfolgen kann. Dieser sollte bei seiner Entlassung hierzu befragt werden. Sollte er mit einer Löschung nicht einverstanden sein, sollten die Daten nach fünf Jahren gesperrt werden. Diese Datensperre darf nur aus überwiegenden Gründen des Gemeinwohls oder mit Einwilligung des Betroffenen aufgehoben werden.

Die in Personalneben- oder beiakten geführten Unterlagen sind bei Entlassung des Gefangenen zur Personalakte zu geben oder zu vernichten.

b) Gefangenenkartei

Die Löschungsregelungen, die die Personalakte betreffen, müssen auch für die Gefangenenkartei entsprechend gelten. Im Zuge der Automatisierung der Gefängnisverwaltung wird sie ohnehin ihre Funktion verlieren, auf die Führung einer manuellen Gefangenenkartei könnte dann verzichtet werden. Nach der Entlassung des Gefangenen sollten die Karteikarten, bei automatisierter Führung ein Ausdruck, zur Personalakte genommen werden. Soweit erforderlich kann ein nur dem Auffinden der Akten dienendes gesondertes Nachweissystem aufgebaut werden.

c) Krankenakte

Die Krankenakte ist von der Personalakte strikt zu trennen. Entsprechend der Regelung der Nr. 60 VGO ist sicherzustellen, daß die Krankenakte beim Anstaltsarzt aufbewahrt wird. Der Betroffene kann sich dann auch nach seiner Entlassung bei Bedarf unmittelbar an den untersuchenden und behandelnden Anstaltsarzt wenden. Der Aufbewahrungszeitraum für die Krankenakte sollte den allgemeinen Regelungen der Aufbewahrungsfrist von ärztlichen Unterlagen entsprechen (Berufsordnung für Ärzte). Nach Entlassung des Gefangenen sollte seine Krankenakte sofort gesperrt werden.

d) Verschiedene Buchwerke

Zugangs- und Abgangsbuch mit personenbezogenen Daten der Strafgefangenen sind nach gesetzlich vorgeschriebener Frist zu vernichten. Die Bücher sollten dem jeweiligen Abschlußzeitraum angepaßt werden. Nach Abschluß dieses Zeitraums ist die namentliche Dokumentation der Häftlinge in diesen Büchern nicht mehr erforderlich, sie sollten gesperrt werden. Sobald die Bücher in automatisierter Form geführt werden, ist der jeweils für den Einzelfall früheste Löschungstermin vorzusehen.

Für die Krankenbücher sind entsprechende Regelungen vorzusehen. Sie sind nach ihrem Abschluß dem Anstaltsarzt auszuhändigen. Die verschiedenen Kalender, in denen Termine der Gefangenen vermerkt sind, verlieren ihre Funktion am Jahresende. Sie sind zu sperren, ihre baldmögliche Löschung ist vorzusehen.

e) Weitere Datensammlungen, wie Sammelakten, Besucherkartei, Störerkartei usw. sind mit der Entlassung der Gefangenen zu löschen oder zur Personalakte zu nehmen. Daten Dritter sollten möglichst zeitig gelöscht werden. Soweit eine längere Aufbewahrung von Besucherdaten erforderlich sein sollte, sollten sie in der Regel nach einem Jahr, in besonderen Fällen spätestens nach zwei Jahren gelöscht werden.

f) Bei der Einführung automatisierter Datenverarbeitungssysteme sind die technischen und organisatorischen Datenschutzmaßnahmen zu treffen. Insbesondere wird darauf hingewiesen, daß die relevanten Datenverarbeitungsvorgänge zu protokollieren sind (§ 9 Abs.1 Nr. 7 LDatG). Die flexiblen Gestaltungsmöglichkeiten der automatisierten Datenverarbeitung sind zu nutzen, indem differenzierte Zugriffs- und Löschungsregelungen eingeführt werden.

Es ist sicherzustellen, daß Mitgefangene keine Einsichtmöglichkeiten auf die Bildschirme bekommen. Insgesamt ist zu gewährleisten, daß Dritte keine unnötige Kenntnis von der Inhaftierung erhalten. Nach Ausscheiden des Gefangenen aus dem Strafvollzug sind seine Daten im automatisierten Verfahren – bis auf einen unerläßlichen Rumpfdatenbestand bzw. Aktennachweis – zu löschen. Ein Ausdruck oder Teilausdruck der zuletzt gespeicherten Daten kann zur Personalakte genommen werden, soweit die weitere Aufbewahrung erforderlich ist. Die Daten, die über den Entlassungstermin hinaus gespeichert werden, sollten nur einem stark eingeschränkten Personenkreis (bzw. allein dem Anstaltsleiter) zugänglich sein.