



104 Seiten

Bericht

**des Landesbeauftragten für den Datenschutz
bei der Präsidentin des Schleswig-Holsteinischen Landtages**

Fünfzehnter Tätigkeitsbericht

In der Anlage übersende ich gemäß § 23 Abs. 3 Satz 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen vom 30. Oktober 1991 den fünfzehnten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages.

Dr. Helmut Bäuml

13/775

**Der Landesbeauftragte für den Datenschutz
bei der Präsidentin des Schleswig-Holsteinischen Landtages**

Düsternbrooker Weg 82, 2300 Kiel 1
Telefon: 0431/596-3280, Telefax: 0431/596-3300

Der Landesbeauftragte
für den Datenschutz:

Dr. Helmut Bäumler

Dienstzimmer:

2300 Kiel 1, Düsternbrooker Weg 82

Dienstanschluß:

0431/596-3280

Vorzimmer:

Monika Harks
App. 3281

Vertreter
des Landesbeauftragten
für den Datenschutz:

Eckhard Beilecke
App. 3285

Referat LD 1

Dr. Helmut Bäumler
App. 3280

Regina Müller-Kronbügel
App. 3291

Monika Harks
App. 3281

Grundsatzfragen des Datenschutzes

Vorbereitung der Sitzungen der Konferenz
der Datenschutzbeauftragten

Allgemeine Verwaltungsangelegenheiten der Dienststelle

Öffentlichkeitsarbeit, Vorbereitung von Veranstaltungen

Vorbereitung von Publikationen

Fortbildung

Referat LD 2

Eckhard Beilecke
App. 3285

Jürgen von der Ohe
App. 3287

NN
App.

Dörte Neumann
App. 3297

Sandra Meier
App. 3299

Anke Tuschik
App. 3299

Datenschutz im Bereich des Personal-, Wahl-, Melde-,
Ausweis-, Kataster-, Ausländer-, Kommunal-, Gewerbe-,
Bau- und Wirtschaftsverwaltungswesens

Datenschutz im Bereich der Parlamentsverwaltung

Datenschutz im Bereich des Statistik-, Verkehrs-,
Umweltschutz-, Planungswesens und im Kulturbereich
sowie in Bereichen, für die keine andere Zuständigkeit festgelegt ist

Dokumentation, Registratur, Sekretariat

Referat LD 3

Uwe Jürgens

App. 3295

Heiko Behrendt

App. 3294

Datenschutz im Bereich der Steuer- und Landwirtschaftsverwaltung

Grundsatzfragen der Datensicherung und der ordnungsgemäßen Anwendung der DV-Programme (§§ 7, 8 LDSG), Prüfungen von Rechenzentren, Prüfung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind.

Mitwirkung bei der Erstellung von Gutachten

Neue Medien und Informationstechniken, Medienrecht

EDV-Einsatz der Dienststelle

Führung und Veröffentlichung der Dateienübersicht, § 24 LDSG

Referat LD 4

Herbert Neumann

App. 3290

Gabriele Meyer-Bettyn

App. 3286

Hans-Jürgen Strasdat

App. 3296

Datenschutz im Sozial-, Wissenschafts-, Forschungs- und medizinischen Bereich

Datenschutz im Justiz-, Polizei- und Verfassungsschutzbereich

FÜNFZEHNTER TÄTIGKEITSBERICHT
des Landesbeauftragten für den Datenschutz
bei der Präsidentin
des Schleswig-Holsteinischen Landtages

nach § 23 Abs. 3 des
Schleswig-Holsteinischen Gesetzes
zum Schutz personenbezogener Informationen
vom 30. Oktober 1991

(Berichtszeitraum: März 1992 bis Februar 1993)

Inhaltsverzeichnis	Seite
1. Zur Lage des Datenschutzes in Schleswig-Holstein	9
1.1 Wechsel im Amt des Datenschutzbeauftragten	9
1.2 Die Möglichkeiten der Dienststelle	9
1.3 Die Reaktion der Verwaltung auf die Kontrollen des Landesbeauftragten für den Datenschutz	10
1.4 Die Reaktion der Verwaltung auf das neue Landesdatenschutzgesetz	11
2. Die verfassungsrechtliche Dimension des Datenschutzes	12
2.1 Der unaufhaltsame Prozeß der Automatisierung	12
2.2 Der Abbau von Grundrechten	14
2.3 Datenschutz und Informationsrechte	16
3. Datenschutz im Parlament	18
3.1 Information des Landtages, seiner Ausschüsse und einzelner Abgeordneter	18
3.2 Schutz der Abgeordnetendaten	20
4. Datenschutz in der Verwaltung	21
4.1 Allgemeine und innere Verwaltung	21
4.1.1 Personalwesen	21
4.1.1.1 Teilnahme des Personalrats an Sitzungen der Gemeindevertretung	21

	Seite
4.1.1.2 Teilnahme der Schwerbehindertenvertretung an den Sitzungen des Präsidialrates eines Gerichtes	22
4.1.1.3 Wofür ein öffentlich Bediensteter einstehen muß	22
4.1.1.4 Führung von Personalakten über Referendare verbesserungsbedürftig	24
4.1.1.5 Kultusministerin reagiert auf Prüfbericht	26
4.1.2 Verfassungsschutz	27
4.1.3 Öffentliche Sicherheit	27
4.1.3.1 Das neue Landesverwaltungsgesetz	27
4.1.3.2 Konsequenzen aus der Datenschutzprüfung bei der Polizei weiterhin unbefriedigend	29
4.1.3.3 Neuregelung der Lichtbildvorzeigekartei	33
4.1.3.4 In den Mühlen der Sicherheitsbürokratie	34
4.1.3.5 Sensible Daten über die Familien von Ausreißern	36
4.1.3.6 Wozu das Paßfoto noch von Nutzen sein kann	37
4.1.4 Ausländerwesen	38
4.1.4.1 Neufassung des Asylverfahrensgesetzes	38
4.1.4.2 Müssen sich Asylbewerber selbst strafbarer Handlungen bezichtigen?	39
4.1.5 Bau- und Wohnungswesen	40
4.2 Kommunalrecht	41
4.2.1 Erste Erfahrungen bei der Anwendung des neuen Datenschutzrechts	41
4.2.1.1 Einführung einer Sozialstaffel für Elternbeiträge im Kindergarten	42
4.2.1.2 Führung eines kommunalen Grundstückseigentümerverzeichnis und Zweckbindung der Daten	42
4.2.1.3 Transparenz der Datenverarbeitung für den Bürger	43
4.2.2 Datenschutz bei Beratungen der Gemeindevertretung: nicht ausgerechnet gegen den Betroffenen	44
4.3 Justizverwaltung	46
4.3.1 Geltung des Landesdatenschutzgesetzes im Justizbereich	46
4.3.2 Geschäftsstellenautomation der Staatsanwaltschaft (GAST): Verbesserungen werden wirksam	49
4.3.3 Konsequenzen aus den Kontrollen in Justizvollzugsanstalten kommen in Gang	51
4.3.4 Was Gefangene über ihr Wachpersonal in Erfahrung bringen konnten	54
4.3.5 Mehr Datenschutz für Zeugen	55
4.3.6 Risiken bei der Genomanalyse in Strafverfahren	56
4.3.7 Mitteilungen in Strafsachen: Gesetz läßt weiter auf sich warten	58

	Seite	
4.3.8	Datenschutzrechtliche Probleme beim Grundbuch	58
4.4	Steuerverwaltung	59
4.4.1	Was hat der Name des Hypothekengläubigers mit der Höhe eines Einheitswertes zu tun?	59
4.4.2	Datensicherheit für Akten und sonstige Unterlagen	60
4.5	Wirtschaft, Technik und Verkehr	62
4.6	Sozial- und Gesundheitswesen	63
4.6.1	Sozialwesen	63
4.6.1.1	Datenerhebung beim Betroffenen oder Amtsermittlung?	63
4.6.1.2	Grenzen der Datenerhebung durch das Sozialamt	64
4.6.1.3	Keine Amtshilfe für die Telekom	65
4.6.1.4	Stichprobenprüfungen in Sozialämtern	65
4.6.2	Gesundheitswesen	68
4.6.2.1	Abgleich von Betäubungsmittelrezepten eines Gesundheitsamtsbezirks	68
4.6.2.2	Weitergabe amtsärztlicher Gutachten ohne Einwilligung des Betroffenen	69
4.6.2.3	Änderungen im Gesundheitsrecht	70
4.7	Kultusbereich	72
4.7.1	Studentendatenverordnung	72
4.7.2	Umfragen durch Elternvertretungen	73
4.7.3	Aufbewahrung von Klassenarbeiten	74
4.7.4	Bekanntgabe von Zensuren in der Klasse	74
4.7.5	Klassenbücher einst und heute	75
4.8	Landwirtschaftsverwaltung	76
4.8.1	Neues Förderungssystem, perfekte Kontrolle	76
4.8.2	Fehler, die sich nicht bezahlt machen	78
5.	Datenschutz bei den Gerichten	80
5.1	Datenschutzrechtliche Beratung von Gerichten	80
5.2	Anspruch auf rechtliches Gehör contra Datenschutz	81
6.	Ordnungsmäßigkeit der Datenverarbeitung	82
6.1	Prüfungen im Bereich der automatisierten Datenverarbeitung	82
6.1.1	Erst ins Wasser springen, dann das Schwimmen lernen?	82
6.1.2	Die automatisierte Datenverarbeitung einer Großstadt	85
6.1.3	Datenschutzrechtliche Forderungen aus einer Prüfung im Jahr 1989 werden noch immer abgearbeitet	89

	Seite
6.2 Beachtung der neuen Sicherheits- und Ordnungsmäßigkeitsvorschriften	91
6.2.1 Alle warten auf die Datensicherungsverordnung	91
6.2.2 Datenverarbeitende Stellen versäumen Übersendung der Dateibeschreibungen	92
6.2.3 Geräteverzeichnisse – mehr als bloße Formalität?	93
6.2.4 Kein Datenschutz beim Funkverkehr?	94
6.3 Aus der Arbeit der IT-Kommission des Landes und der Automationskommission der Kommunen	96
6.3.1 Musterregelung für den Einsatz privater Personalcomputer	96
6.3.2 Mindestanforderungen an die Verfahrensdokumentation in Kraft	97
6.3.3 Die IT-Verfahrensregelung wird nicht immer beachtet	98
6.3.4 Richtungsweisende Empfehlungen der Automationskommission der Arbeitsgemeinschaft der kommunalen Landesverbände	99
6.4 Was IT-Führungskräfte wissen sollten	101

1. Zur Lage des Datenschutzes in Schleswig-Holstein

1.1 Wechsel im Amt des Datenschutzbeauftragten

Zum 1. September 1992 ist **Ernst Eugen Becker** nach 14jähriger Tätigkeit als Landesbeauftragter für den Datenschutz in den Ruhestand getreten. Er hat das Amt aufgebaut und ihm in den schwierigen Anfangsjahren ein solides Fundament gegeben. Seine Art, die Dinge anzugehen, hat dem Datenschutz innerhalb und außerhalb von Schleswig-Holstein Respekt und Anerkennung eingebracht. Zu Recht haben deshalb die Repräsentanten des Landes Person und Leistung von Ernst Eugen Becker bei seiner Verabschiedung gewürdigt. Mit ihm ist ein konsequenter, wenngleich nie lautstark auftretender Verfechter des Datenschutzes gegangen. Er hat die Höhen und Tiefen des Amtes durchlebt, die Diskussion um die Volkszählung aktiv mitgestaltet und auf seine Art und Weise die Datenverarbeitung im Lande im Interesse der Bürgerinnen und Bürger und der Wahrung ihrer Rechte nachhaltig beeinflusst. Seine Mitarbeiter verdanken ihm viele Jahre angenehmer, konstruktiver und effektiver Zusammenarbeit.

Der **Landtag** hat mich mit **großer Mehrheit** zum **neuen Landesbeauftragten für den Datenschutz gewählt**. In der parteiübergreifenden Zustimmung sehe ich eine besondere Ermutigung, das Amt konsequent und im Interesse aller Bürger auszuüben. Die dabei notwendigerweise auftretenden Streitfragen mit den datenverarbeitenden Stellen müssen ausgetragen werden. Ich setze aber gleichermaßen auf die Kooperation mit der Verwaltung. Sie muß nicht nur um der gesetzlichen Verpflichtung willen, sondern auch im eigenen Interesse für die Beachtung des Datenschutzes sorgen.

Insofern knüpfe ich da an, wo mein Vorgänger aufgehört hat. Natürlich möchte ich auch neue Akzente setzen, wo es mir von der Sache her geboten erscheint. In diesem Bericht, der zur Hälfte noch die Amtszeit meines Vorgängers betrifft, klingt das eine oder andere bereits an. An einigen Stellen mag auch das „Wir“ ins Auge springen, mit dem zum Ausdruck kommen soll, daß in der Dienststelle des Landesbeauftragten auch in Zukunft Teamarbeit geleistet werden soll.

1.2 Die Möglichkeiten der Dienststelle

Über die **Personalausstattung** der Dienststelle ist im letzten Tätigkeitsbericht Klage geführt worden. Im Grunde hat sich an der Situation seitdem nichts Entscheidendes geändert. Immerhin konnte im Berichtsjahr eine neue Sachbearbeiterstelle besetzt werden; für 1993 besteht begründete Hoffnung auf Bewilligung einer weiteren Sachbearbeiterstelle durch das Parlament. Beide Male muß aber ein erheblicher Teil der Mehrkosten durch Einsparung an anderer Stelle des Haushalts erwirtschaftet werden, was bei einem kleinen Haushalt wie dem der Dienststelle zu kaum lösbaren Problemen führt.

Da eine **wirksame Außenkontrolle** bei den vielen datenverarbeitenden Stellen im Lande nur sporadisch möglich ist, kommt es auf eine **sorgsame Auswahl der zu kontrollierenden Stellen** an. Sie müssen repräsentativ für die Datenverarbeitungspraxis sein. Für die Beseitigung der bei den Kontrollen aufgedeckten Schwachstellen ist langer Atem notwendig, damit der Kontrollaufwand lohnt. Es muß angestrebt werden, die Ergebnisse von Kontrollen zu verallgemeinern, wo immer dies möglich ist. Es gilt aber auch, die Seite der **Prävention** zu verstärken. Deshalb stehen neben der Kontrolle **Aufklärung und Fortbildung** im Mittelpunkt der Arbeit. Kurz nach Inkrafttreten des neuen Landesdatenschutzgesetzes (LDSG) wurden Woche für Woche Behördenmitarbeiter ins Landeshaus nach Kiel zu eintägigen Fortbildungsveranstaltungen eingeladen. Insgesamt wurden 18 Tagesseminare mit 540 Teilnehmern, zumeist Multiplikatoren, durchgeführt. In ungezählten Vertragsveranstaltungen wurden darüber hinaus vor Ort den unterschiedlichsten Teilnehmerkreisen die Grundzüge des neuen Datenschutzrechts erläutert.

Ausgehend von dem erfolgreichen Datenschutztag im Kieler Landeshaus wurde mit der Veranstaltung **regionaler Datenschutztage** in den Kreisen und den kreisfreien Städten begonnen. In Lübeck und Husum hat die Dienststelle einen ganzen Tag lang in den dortigen Rathäusern in Vorträgen, Arbeitsgruppen, Podiumsdiskussionen und Einzelgesprächen Hinweise für die praktische Handhabung des Datenschutzrechts gegeben. Die Bürger konnten sich an Ausstellungsständen, in Bürgersprechstunden und im Rahmen von Telefonberatungen über Datenschutz und Datensicherheit und über ihre Rechte informieren.

Die Veranstaltungen haben bei Bürgern, Verwaltung und Presse einen guten Anklang gefunden. Sie sollen 1993 fortgeführt werden. Wir verbinden damit die Hoffnung, daß das Wissen über die datenschutzrechtlichen Rechte und Pflichten bei den Betroffenen dadurch verbreitet wird. Aufklärung und Vorbeugung haben also nicht nur im Gesundheits- und Sicherheitsbereich, sondern auch beim Datenschutz ihren guten Sinn.

1.3 Die Reaktion der Verwaltung auf die Kontrollen des Landesbeauftragten für den Datenschutz

Der Verwaltung wird manchmal nachgesagt, sie arbeite zu langsam. Ob das in dieser Allgemeinheit zutrifft, mag dahinstehen. Würde man die Reaktion auf die Kontrollen des Datenschutzbeauftragten zum Maßstab nehmen, so könnte man sich allerdings leicht zu diesem Schluß verleiten lassen.

Zumeist dauert es schon **Monate**, bis die **ersten Stellungnahmen** zu den Prüfberichten eingehen. Danach beginnen oft zeitraubende Verhandlungen über die strittigen Punkte. Sind die schließlich abgehakt, dann steht die Phase der Realisierung der zugesagten Veränderungen an. Zwischen dem Beginn einer Querschnittskontrolle und der Umsetzung der notwendi-

gen Verbesserungen vergehen so oft Jahre – eine Ewigkeit in den Maßstäben der elektronischen Datenverarbeitung.

Beispiele für die langwierige Umsetzung datenschutzrechtlicher Anforderungen finden sich auch in diesem Bericht (Tzn. 4.1.1.5, 4.1.3.2, 4.3.2, 4.3.3, 6.1.3).

Die Gründe für die zögerliche Haltung mancher Behörden in Datenschutzfragen sind vielschichtig. Berichte über Querschnittskontrollen sind häufig umfangreich und berühren viele Aspekte des Verwaltungsvollzugs. Werden grundlegende Veränderungen angemahnt, so mag man sich zweimal überlegen, wie die Sache angepackt werden soll. Dies und das kann im Einzelfall hinzukommen und die Verzögerung plausibel erscheinen lassen. Gelegentlich mag auch das lautstarke Klagen über zuviel Datenschutz davon abhalten, daß tatsächlich etwas für den Datenschutz der Bürger getan wird.

Alles in allem ist kaum vorstellbar, daß die Verwaltung auch im übrigen so zögerlich bei der Umsetzung von Gesetzen ist. Es ist also eine Frage der **Prioritäten**, die man setzt. Besonders ins Auge springt die Kontrolle der Datenverarbeitung bei der **Polizei**. Sie wurde 1988 durchgeführt. Unter Tz. 4.1.3.2 ist nachzulesen, wie sich der Stand der Dinge gegenwärtig darstellt und welchen Kritikpunkten inzwischen Rechnung getragen ist. Zu wenig, gemessen an der Bedeutung der polizeilichen Datenverarbeitung für das Recht auf informationelle Selbstbestimmung.

Gewiß, die Polizei muß primär Gefahren abwehren und Straftaten aufklären, der Justizminister muß den ordnungsgemäßen Betrieb der Vollzugsanstalten sicherstellen, die Datenzentrale muß Daten verarbeiten usw. Aber alle dürfen es nur unter Einhaltung der Gesetze, einschließlich des Datenschutzrechts.

1.4 **Die Reaktion der Verwaltung auf das neue Landesdatenschutzgesetz**

Das neue LDSG ist nun seit über einem Jahr in Kraft. Natürlich ist es noch zu früh, ein fundiertes Urteil über seine Akzeptanz und Beachtung bei der Verwaltung zu treffen.

Über **erste Erfahrungen** mit dem neuen Gesetz, die aus der Verwaltung berichtet wurden, ist an anderer Stelle (vgl. Tzn. 4.2.1, 4.6.1.4, 6.2.2) nachzulesen. Bereits im Herbst des Berichtsjahres haben wir einige **ausgewählte Bereiche stichpunktartig überprüft** und dabei einzelne Mängel bei der Anwendung des neuen Gesetzes festgestellt. Im großen und ganzen sind aber noch keine gravierenden Unzuträglichkeiten zutage getreten. Vermutlich gibt es aber eine hohe Dunkelziffer an datenschutzrechtlichen Verstößen, und sei es aus Unkenntnis der Vorschriften. Aus der bisher nur zögerlich erfolgenden Anmeldung neuer automatisierter und insbesondere der ausbleibenden Nachmeldung manueller Karteien läßt sich der Schluß ziehen, daß trotz aller Aufklärung bei vielen Stellen noch Unkenntnis über die praktischen Auswirkungen des

neuen LDSG herrscht. Weitere Kontrollen werden im laufenden Jahr diesbezüglich mehr Klarheit schaffen.

Wir haben im vergangenen Jahr umfangreiche **Hinweise** zum neuen LDSG herausgegeben, die im **Amtsblatt** für Schleswig-Holstein (Amtsbl. 1992, S. 753) veröffentlicht wurden. Sie sollen die Handhabung des Gesetzes erleichtern und auslegungsbedürftige Bestimmungen präzisieren.

2. Die verfassungsrechtliche Dimension des Datenschutzes

2.1 Der unaufhaltsame Prozeß der Automatisierung

Nur auf den ersten Blick mag es überraschend sein, in einem Kapitel über die verfassungsrechtliche Fundierung des Datenschutzes Ausführungen über die Entwicklung der **Datenverarbeitungstechnik** zu finden. Aber Technikfragen haben stets auch inhaltliche Implikationen, jedenfalls wenn es um die Verarbeitung personenbezogener Daten geht. Es macht für das Recht auf informationelle Selbstbestimmung einen erheblichen Unterschied, ob Daten in Karteien oder Akten oder „modern“ in einer elektronischen Datenbank verarbeitet werden. So einleuchtend dies ist, so wenig stellen die Datenschutzgesetze auf diesen Aspekt ab. Primärer Regelungsgegenstand ist die Frage, „ob“ dieses oder jenes Datum verarbeitet werden darf, nicht „wie“ dies zu geschehen hat. Nur gelegentlich, etwa bei den Bestimmungen über Online-Datenverarbeitung, setzt das Gesetz an der Technik der Verarbeitung an.

So muß es nicht verwundern, daß Fragen der Automatisierung der Datenverarbeitung selten unter datenschutzrechtlichen, viel häufiger dagegen unter **haushalts- und organisationsrechtlichen Gesichtspunkten** diskutiert werden. Daher wird die Einführung und stetige Optimierung der elektronischen Datenverarbeitung nicht so sehr unter Grundrechtsaspekten gesehen. Finanzierbarkeit und Machbarkeit spielen vielmehr die entscheidende Rolle. Aber auch insoweit wird häufig nicht – wie man erwarten könnte – mit nüchternen Zahlen und kühlem Kopf kalkuliert. Der Wunsch, „konkurrenzfähig“ sein und den Anschluß nicht verpassen zu wollen sowie der unerschütterliche Glaube, die Automatisierung der Datenverarbeitung führe stets, quasi naturgesetzlich, zu Kosteneinsparungen, bestimmen die Diskussion.

Dabei wird häufig übersehen, daß die Anschaffung von Computern allein nicht das Entscheidende ist. Zu ihrer Benutzung müssen Bedienstete aus- und angesichts der ständigen Neuerungen kontinuierlich fortgebildet werden (vgl. Tz. 6.4). Der Wartungsaufwand auch bei neuer Hard- und Software schlägt zu Buche. Computer müssen mit gelegentlich enormem Organisationsaufwand in eine vorhandene Informationsverarbeitungsstruktur eingepaßt oder – häufig – letztere den Computern angepaßt werden. Daß auch Fragen der Ergonomie, der Mitbestimmung und der humanen Gestaltung des Arbeitsplat-

zes berücksichtigt werden müssen, sei nur der Vollständigkeit halber erwähnt. Erstaunt wird dann, wenn die Gelder verplant oder ausgegeben sind, festgestellt, daß man nun auch noch etwas für Datenschutz und Datensicherheit tun muß.

Wird all dies nicht rechtzeitig gesehen, dann stellt sich der **Rationalisierungsgewinn** bei der Automatisierung der Datenverarbeitung freilich zunächst in **rosaroten Farben** dar. Forderungen nach Aufwendungen für die Ordnungsmäßigkeit der Datenverarbeitung, etwa für die Dokumentation der Programme und die Sicherheit der Anlagen, wirken da nur hinderlich. Datenschutz und Datensicherheit geraten dann in die Rolle des Störenfrieds in der heilen Welt der Automatisierung, Rationalisierung, Kosteneinsparung usw.

Dabei geht es keineswegs nur um Fragen der möglichst noch leistungsfähigeren Methode der Datenverarbeitung. Das Bundesverfassungsgericht hat im Volkszählungsurteil deutlich gemacht, daß gerade „unter den Bedingungen der modernen Datenverarbeitung“ die Befugnis des einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, des besonderen Schutzes bedarf. Aber nicht nur im Hinblick auf das Recht des einzelnen, sondern auch für die Wirksamkeit des **demokratischen Rechtsstaats** ist die datenschutzgerechte Gestaltung des Automatisierungsprozesses von elementarer Bedeutung. Wenn die Verarbeitung personenbezogener Daten durch staatliche Stellen immer mehr automatisiert und dadurch komplex und undurchschaubar für den einzelnen wird, wird er es sich zweimal überlegen, ob er seine demokratischen Rechte wahrnimmt. Demokratie gründet sich aber entscheidend auf die aktive Teilhabe der Bürger. So gesehen dient aktiver und effektiver Datenschutz nicht nur dem Individuum, sondern zugleich dem Erhalt der freiheitlichen demokratischen Grundordnung.

Dieser Bedeutung des Datenschutzes wird der **reale Prozeß der Automatisierung** häufig nicht gerecht. Wenngleich die IT-Richtlinien des Landes vorschreiben, daß vor der Einführung neuer Verfahren die datenschutzrechtlichen Fragen zu klären sind, wird die Automatisierung gleichwohl auch dort vorangetrieben, wo es an normenklaren Rechtsgrundlagen für die Datenverarbeitung fehlt. Bestehen einmal vernünftige Leitlinien für den Entscheidungsprozeß bei der Automatisierung, wie etwa die Empfehlungen der Automationskommission der Arbeitsgemeinschaft der kommunalen Landesverbände, dann ist bei den Kontrollen vor Ort wenig davon zu spüren, daß sie tatsächlich beachtet werden (vgl. Tz. 6.3.4).

So schreitet die Automatisierung voran und führt die staatliche Verwaltung immer tiefer in die Abhängigkeit von der elektronischen Datenverarbeitung. Die Risiken der Verletzlichkeit der Informationsgesellschaft werden verdrängt oder den Mahnern wird der „Beweis“ für die Risiken abverlangt. Der Prozeß der Erosion der Grundrechte verläuft aber schleichend und selten spektakulär.

So werden wir uns z.B. wohl auch daran „gewöhnen“, zukünftig verstärkt aus der Luft beobachtet zu werden. Gewiß, Luftaufklärung und Satellitenbeobachtung kannte man aus dem militärischen Sektor. Erstmals soll in der Bundesrepublik und damit auch in Schleswig-Holstein nun aber die **Satellitenbeobachtung zum Verwaltungsvollzug** eingesetzt werden (vgl. Tz. 4.9.1). Der gigantische Subventionsapparat in der Landwirtschaft verlangt nach Kontrolle der ausgeworfenen Gelder. Künftig soll mit Satelliten überwacht werden, ob die Angaben der Bauern in den Subventionsanträgen mit den tatsächlichen Gegebenheiten auf den Feldern übereinstimmen. Wer sollte etwas dagegen haben, wenn die zweckgerechte Verwendung der immensen Subventionssummen, die ja von der Allgemeinheit aufgebracht werden müssen, effektiv kontrolliert wird? Warum soll ein Kontrolleur mühsam durch die Flur stapfen, wo es doch moderner, einfacher und geräuscherloser aus dem Weltall geht? High tech at its best. Ist der Anfang erst einmal gemacht, dann wird die Steuerverwaltung vielleicht auf die Idee kommen, daß es interessant wäre zu wissen, wer einen Swimmingpool im Garten hat, wie viele Autos welcher Marke im Hof stehen, wie viele Yachten im Hafen liegen. Als nächstes könnte die Bauverwaltung entdecken, daß sich Kontrollen bei Bauvorhaben doch ganz gut auch aus der Luft durchführen lassen.

Zukunftsmusik, ohne Zweifel. Aber wer vor Jahren darauf hinwies, daß in der zunehmenden „Leistungsfähigkeit“ der Satellitenaufklärung eines Tages ein Risiko für das Recht auf informationelle Selbstbestimmung liegen könnte, wurde milde belächelt. 1993 könnten wir der Überwachung durch „**big brother**“ aus dem Weltall schon ein ganzes Stück näher kommen. Es sei denn, unsere Bedenken finden doch noch Beachtung.

2.2 Der Abbau von Grundrechten

Wir haben angesichts der technischen Entwicklung allen Anlaß, über die Sicherung und Effektivierung der Grundrechte in einer potentiell grundrechtsfeindlichen Technikwelt nachzudenken. Schon im 14. TB (S. 12) wurde deshalb verlangt: „Mehr Datenschutz ins Grundgesetz.“ Die Arbeiten an der **Reform der Verfassung** im Zuge der Vereinigung Deutschlands wurden im vergangenen Jahr fortgesetzt. Es bestehen nach wie vor gute Chancen, daß auch der Datenschutz dabei Berücksichtigung findet und zumindest der Status quo nach dem Volkszählungsurteil abgesichert wird.

Aber statt angesichts der auf dem Markt befindlichen Geräte zum Belauschen und Beobachten von Wohnungen den Schutz der Privatsphäre im Grundgesetz zu verbessern, wird lauthals die Legalisierung des sog. „**Lauschangriffs**“ verlangt. In bestimmten Fällen soll es zulässig sein, daß in Wohnungen Abhörwanzen angebracht werden und jedes dort geführte Gespräch mitgehört und aufgezeichnet wird. Begründet wird dies mit dem Anwachsen der Kriminalität schlechthin und organi-

sierter Kriminalität im besonderen. Ein Trommelfeuer von Zahlen und Statistiken und bestürzenden Einzelfällen aus Polizeiakten soll Politiker und Gesellschaft reif für die Einführung des Lauschangriffs machen.

Dabei wird so getan, als komme es nur darauf an zu beweisen, daß durch den Lauschangriff Ermittlungserfolge zu erzielen wären, die ohne ihn nicht möglich sind. So als stünden die **Grundrechte zur Disposition**, wenn es ohne sie „besser“ und „einfacher“ ginge. Eine Diskussion, die sich darauf beschränkt, ob der Lauschangriff „etwas bringt“, greift zu kurz. Sie wird dem Umstand nicht gerecht, daß der Schutz der Privatwohnung in engem Zusammenhang mit dem Schutz der Menschenwürde steht, der nach unserer Verfassung unveräußerlich ist. Jeder Mensch braucht einen Ort und eine Sphäre, in der er für sich ist und ungestört von staatlicher Beobachtung kommunizieren kann. Totale Überwachung jeglicher menschlicher Betätigung an jedem Ort wird dem Menschenbild des Grundgesetzes nicht gerecht.

Es fällt auf, daß andere, weniger einschneidende, aber erfolgversprechende gesetzliche Maßnahmen gegen organisierte Kriminalität nicht so recht vorankommen. Die italienischen Ermittler verdanken ihre Erfolge unter anderem auch der Möglichkeit, die **Bankverbindungen** der sizilianischen Mafia zu durchleuchten. Deutschland gilt nach wie vor als ein ideales Land zur Geldwäsche. Ein von der Polizei als wichtig angesehenes Gesetz zur Ermittlung illegaler Geldtransaktionen, das sogenannte „Gewinnaufspürungsgesetz“, wurde aus dem Gesetzespaket zur Bekämpfung der organisierten Kriminalität im vergangenen Jahr im letzten Moment ausgeklammert. Dem Vernehmen nach sollen sich die Banken dagegen gewandt haben. Gelegentlich wird in der Diskussion so getan, als sei das Bankgeheimnis eines der wichtigsten Prinzipien des Datenschutzes. Dabei ist es weder in der Konvention des Europarats noch in anderen Gesetzen als besonders sensibles Datum aufgeführt. Millionen von Bankkunden müssen notgedrungen einwilligen, daß ihre finanziellen Verhältnisse bei der Schufa gespeichert und auf Anfrage an die Banken und die Kreditwirtschaft übermittelt werden. Eine Durchleuchtung der großen Geldtransaktionen zur Bekämpfung der Geldwäsche würde also aus datenschutzrechtlicher Sicht nicht auf unüberwindliche Hindernisse stoßen.

Natürlich wollen die Befürworter des Lauschangriffs nicht den **Überwachungsstaat**. Sicher sind ihre Argumente schwerwiegend, ist die Gefahr des organisierten Verbrechens für Staat und Gesellschaft real. Zweifellos würde sich der Lauschangriff zunächst nur gegen Verdächtige richten, die schwere Straftaten begangen haben oder weiter begehen wollen.

Aber gewisse Grenzen darf man nicht überschreiten, weil dann auch andere Dämme brechen. Ist der Anfang erst einmal gemacht, werden weitere Beobachtungslücken „geschlossen“. Haben sich die Verdächtigen auf die neue Gesetzeslage eingestellt – was bei organisierten Verbrechern sehr schnell der Fall

sein dürfte – muß der Kreis der abzuhörenden Wohnungen erweitert werden. Letztlich wird dann jede Wohnung betroffen sein, von der anzunehmen ist, daß in ihr Absprachen, Planungen etc. für schwere Straftaten vorgenommen werden. Auf der Suche nach noch effektiveren Fahndungsmethoden wird sich die **Spirale der Grundrechtseinschränkungen** unaufhaltsam weiterdrehen.

Deshalb sollten bestimmte **Schwellen** von vornherein nicht überschritten werden. Grundrechte müssen sich vor allem dann bewähren, wenn die Versuchung groß ist, „effektiver arbeiten“, „Chancengleichheit“ mit dem organisierten Verbrechen herstellen und dafür die Verfassung „flexibler“ gestalten zu wollen. Angesichts der rasanten Entwicklung der elektronischen Datenverarbeitung und der technischen Mittel zur optischen und akustischen Überwachung brauchen wir nicht weniger, sondern mehr grundrechtlichen Datenschutz.

2.3 Datenschutz und Informationsrechte

Bei oberflächlicher Betrachtung scheint der Datenschutz neben seiner eigentlichen Funktion auch ein hervorragendes Instrument zur Abschottung, Heimlichtuerei und Vertuschung eigener Fehler zu sein.

Häufig werden – auch berechtigte – Informationsansprüche unter pauschalem Hinweis auf „den Datenschutz“ abgewiesen. Aus einem Schutzrecht für Personen mutiert der Datenschutz dabei unter der Hand zu einem Schutz der Verwaltung oder von Organisationen vor unangenehmen Wahrheiten. Dabei weist schon das Volkszählungsurteil des Bundesverfassungsgerichts den Weg zu einer Interpretation, die individuellem **Datenschutz und Transparenz** staatlichen Handelns gleichermaßen gerecht wird. Wenn nämlich das Recht auf informationelle Selbstbestimmung nicht nur dem Schutz des Individuums dient, sondern auch die Funktionsbedingungen für eine freiheitliche Demokratie sichern soll, dann verbietet sich eine Auslegung, die beide Schutzziele gegeneinander ausspielt.

Elementare Funktionsbedingung für die aktive **demokratische Teilhabe** ist nicht nur der Schutz der eigenen Daten und die Kenntnis der Bedingungen für ihre Verarbeitung, sondern auch die Kenntnis über das staatliche Handeln ohne Bezug zu den eigenen Daten. Es wäre fatal, wenn die gleichen Bedingungen, die zu immer mehr und immer intensiverer Verarbeitung personenbezogener Daten über den Bürger führen, zugleich der **Abschottung der Verwaltung** vor Kontrolle und öffentlicher Teilhabe dienen.

Datenschutz für den einzelnen und legitime Transparenzansprüche gehören also zusammen und dürfen nicht auseinanderdividiert werden. Es mag etwas vereinfacht formuliert sein, bringt aber gleichwohl die Sache anschaulich auf den Begriff, wenn man davon spricht, der „**gläserne Bürger**“ müsse ver-

hindert und zugleich die „**gläserne Verwaltung**“ angestrebt werden.

Während in den USA mit dem **Informationsfreiheitsgesetz** bereits gute Erfahrungen gesammelt werden konnten, ist bei uns die Rechtsentwicklung noch im Fluß. Aber wenn nicht alles täuscht, führt eine Entwicklungslinie von der Einsicht in die gerichtlichen Unterlagen und der Akteneinsicht im Verwaltungsverfahren über den datenschutzrechtlichen Auskunftsanspruch des Betroffenen auch außerhalb des Verwaltungsverfahrens hin zu einem allgemeinen Informationsanspruch auch ohne Bezug zu eigenen Daten. Wichtige Stationen auf diesem Weg sind das **Archivgesetz**, das die Nutzung von Unterlagen zumindest nach Ablauf von Fristen gestattet, und das Recht auf **Einsicht in umweltrelevante Akten**, das sich aus einer Richtlinie des Rates der EG seit Anfang des Jahres unmittelbar ergibt.

Eine weitere Facette des Problems sind die Informationsansprüche des **Parlaments** gegenüber der **Regierung**, über die an anderer Stelle näher berichtet wird (vgl. Tz. 3.1).

Wenn auch letztlich Datenschutz und Transparenz- und Informationsansprüche **zwei Seiten einer Medaille** sind, so können beide ohne Zweifel im Einzelfall in Kollision miteinander geraten. Die Lösung des Konflikts kann nicht in dem einseitigen Vorrang des einen Prinzips gegenüber den anderen bestehen, sondern muß beiden Zielen gerecht werden. Dabei ist eine Verfahrensweise gefordert, die beide Prinzipien möglichst umfassend und effektiv zur Geltung bringt. Wo Sachinformationen von personenbezogenen Daten getrennt werden können, ist dem Informationsanspruch zu genügen und zugleich dem Schutz der personenbezogenen Daten Rechnung zu tragen.

Um Zielkonflikten möglichst von vornherein vorzubeugen, empfiehlt es sich, Datenschutz und Transparenzansprüchen durch eine **geeignete Datenorganisation** Rechnung zu tragen. Werden personenbezogene Daten und Sachinformationen voneinander getrennt, wo dies möglich ist, entfallen bei der Geltendmachung von Akteneinsichtsrechten arbeits- und zeitaufwendige Prozeduren.

3. Datenschutz im Parlament

3.1 Information des Landtages, seiner Ausschüsse und einzelner Abgeordneter

„Darf eine **Kleine Anfrage** über namentlich benannte Personen öffentlich im Landtag behandelt werden?“ „Verstößt es gegen den Datenschutz, wenn dem Finanzausschuß finanzielle Zuwendungen mit den Namen der Zuwendungsempfänger mitgeteilt werden?“ Solche Fragen zeigten auch 1992 wieder, daß Umfang und Grenzen der **Informationspflicht** der Regierung gegenüber dem Parlament noch nicht exakt festgelegt sind. Auch in Zukunft wird von Fall zu Fall eine sorgfältige Prüfung notwendig bleiben. Das Informationsrecht des Landtags und des einzelnen Abgeordneten, das aus den verfassungsgemäßen Aufgaben des Parlaments folgt, kann in Konkurrenz zu dem ebenfalls von der Verfassung garantierten informationellen Selbstbestimmungsrecht des einzelnen Bürgers treten. Beide Rechte müssen in der Praxis in einer Weise aufeinander abgestimmt werden, daß sie in weitestgehendem Umfang wirksam werden können.

In der **Landesverfassung** kommt die erforderliche Interessensabwägung deutlich zum Ausdruck. Von der grundsätzlichen Informationspflicht der Landesregierung sind Ausnahmen zu machen, „... wenn ... schutzwürdige Interessen einzelner, insbesondere des Datenschutzes, entgegenstehen, ...“. Die Öffentlichkeit ist bei Ausschußsitzungen auszuschließen, „... wenn schutzwürdige Interessen einzelner dies erfordern“.

Diese „Datenschutzklauseln“ können in der Praxis allerdings zu unterschiedlichen Ergebnissen führen. Zwei Beispiele zeigen die Bandbreite der Möglichkeiten:

Werden z.B. die Namen von **Sachverständigen** oder **Gutachtern** in öffentlichen Erörterungs- oder Verhandlungsterminen ohnehin bekannt, so können sie keinen Anspruch darauf erheben, daß im Zusammenhang mit parlamentarischen Diskussionen und Anfragen ihre Namen vertraulich behandelt werden. Für Einzelheiten einer Arztrechnung, die Mitarbeiter für Zwecke der Beihilfegewährung einreichen, gilt das dagegen sicher nicht.

Das Schutzbedürfnis hängt auch von der Art der parlamentarischen Behandlung solcher Informationen ab. Personenbezogene Daten sind um so schutzbedürftiger, je stärker die Wahrscheinlichkeit ihrer ungesteuerten Verbreitung in der Öffentlichkeit ist. Informationensuchen des **Eingabenausschusses** wird von der Verwaltung in weitem Umfang entsprochen werden dürfen. Seine Beratungen sind nicht öffentlich und erfolgen grundsätzlich mit Einwilligung des Betroffenen. Die beteiligten Stellen sind nach der Geheimschutzordnung des Landtages und anderen Vorschriften zur Verschwiegenheit verpflichtet.

Untersuchungsausschüsse haben ebenfalls ein weitgehendes Informationsrecht, das sich im wesentlichen nach der Straf-

prozeßordnung bemißt. Schon vom Gewicht ihrer Aufgabenstellung her wird ihrem Anspruch auf ausreichende Unterrichtung dem Grunde nach Vorrang vor den Diskretionsansprüchen Betroffener eingeräumt werden müssen. Hinzu kommt, daß für die Beweisaufnahme eines Untersuchungsausschusses die Öffentlichkeit ausgeschlossen werden kann (und unter Umständen muß), die Beratung selbst unter Ausschluß der Öffentlichkeit stattfindet und Vertraulichkeit nach der Geheimschutzordnung zu wahren ist.

Die **allgemeine Informationspflicht** der Landesregierung gegenüber dem Landtag über Gesetzgebungsvorhaben und Grundsatzfragen dürfte dagegen meist auch ohne Informationen über natürliche Personen möglich sein.

Bei **parlamentarischen Anfragen** ist zu bedenken, daß die Antworten Inhalt einer amtlichen Parlamentsdrucksache und damit öffentlich werden. Häufig muß die Mitteilung personenbezogener Informationen mit Rücksicht auf diese Veröffentlichung unterbleiben. Die Abgeordneten können dann statt dessen auf die Möglichkeit der Akteneinsicht verwiesen werden.

Andere Gesichtspunkte können zum Tragen kommen, wenn – nicht unmittelbar zum Problembereich des Datenschutzes gehörend – Informationen über Verbände oder Juristische Personen in Frage stehen. Um für die Regierung mehr Sicherheit im Umgang mit personenbezogenen Daten gegenüber dem Landtag und für die Betroffenen mehr Transparenz über die parlamentarische Behandlung ihrer personenbezogenen Informationen zu erreichen, sollten die Anstöße der Landesverfassung zur Gesetzgebung aufgegriffen werden. Es liegt im Interesse des Datenschutzes und dürfte auch der Rechtssicherheit aller Beteiligten dienen, wenn ein „**Parlamentsinformationsgesetz**“ derartige Verfahrensregelungen bringt.

Solange ein solches Gesetz noch nicht gilt, muß die datenverarbeitende Stelle der Landesregierung die schutzwürdigen Interessen der Betroffenen im Einzelfall prüfen. Nach unserer Auffassung müßten folgende Schritte vor der Information eines Landtagsausschusses eingehalten werden:

- Bei Abschluß bedeutenderer Vereinbarungen sollten die Vertragspartner des Landes auf die Möglichkeit parlamentarischer Erörterungen ihrer Daten insbesondere im Rahmen von Haushaltsberatungen hingewiesen werden. Ihre generelle Einwilligung in Datenübermittlungen an den Landtag und seine Mitglieder sollte Bestandteil der Absprachen werden. Die Finanzministerin hat das bereits in ihrem Erlaß über die vorläufige Haushaltsführung für 1993 verbindlich vorgeschrieben.
- Liegt ein solches generelles Einverständnis nicht vor, so hat die Landesregierung in eigener Verantwortung abzuwägen, ob der Persönlichkeitsschutz des einzelnen gegenüber dem Informationsanspruch des Parlaments Vorrang genießt.

- Überwiegen die schutzwürdigen Belange Betroffener oder sind mit vorzulegenden Informationen personenbezogene Daten verbunden, die für die Information des Landtages nicht erforderlich sind, so sind diese Daten vor der Information abzutrennen.
- Ist eine Trennung nur mit erheblichem Aufwand möglich, so soll der Ausschußvorsitzende gebeten werden, auf die Einhaltung der Vorschriften der Geheimschutzordnung in besonderem Maße zu achten und die Öffentlichkeit bei der Beratung der Information auszuschließen.
- Kommt die datenverarbeitende Stelle bei der Rechtsgüterabwägung schließlich zu dem Ergebnis, schutzwürdige Interessen Betroffener stünden einer Aktenvorlage nicht entgegen, so bedarf es keiner zusätzlichen Einwilligung der Betroffenen.
- Eine solche Einwilligung kann nach alledem nur in Betracht gezogen werden, wenn Gründe des informationellen Selbstbestimmungsrechts die Ablehnung einer Aktenvorlage gebieten, andere Gründe sie aber wünschenswert erscheinen lassen. In diesem Fall kann nur der Betroffene selbst über die Geltendmachung seiner Rechte entscheiden.

3.2 Schutz der Abgeordnetendaten

Datenschutz im Parlament betrifft auch den Umgang des Landtags mit den Daten seiner Mitglieder. Die „**Verhaltensregeln für Abgeordnete**“ sehen die Verarbeitung umfangreicher Daten über Abgeordnete vor. Wir hatten zu entsprechenden Entwürfen schon vor einigen Jahren Stellung genommen. Der materielle Inhalt dieser Vorschriften entzieht sich aus verfassungsrechtlichen Gründen unserer Beurteilung.

Die formellen Vorschriften entsprechen weitgehend den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts. Zweck und Inhalt der Datenverarbeitung werden beschrieben, die Befugnis zur Datenverarbeitung und die Zuständigkeit werden festgelegt. Nach dem Abgeordnetengesetz sind weiter von der Landtagsverwaltung **technische und organisatorische Maßnahmen** für den sorgsam und zurückhaltenden Umgang mit den Daten der Abgeordneten zu treffen. Die Verabschiedung der Verhaltensregeln könnte Gelegenheit sein, die erforderlichen Ausführungsbestimmungen nunmehr ebenfalls zu erlassen und damit den praktischen Umgang mit den personenbezogenen Daten der Abgeordneten zu regeln.

- 4. **Datenschutz in der Verwaltung**
- 4.1 **Allgemeine und innere Verwaltung**
- 4.1.1 **Personalwesen**
- 4.1.1.1 **Teilnahme des Personalrats an Sitzungen der Gemeindevertretung**

Soweit mitbestimmungspflichtige Angelegenheiten beraten werden, hat der Personalrat ein Recht auf Teilnahme an Sitzungen der Gemeindevertretung und ihrer Ausschüsse, auch wenn die Öffentlichkeit ausgeschlossen ist. Die erforderlichen Sitzungsunterlagen sind ihm zugänglich zu machen.

Hat der Personalrat ein Recht auf Teilnahme an **nichtöffentlichen** Sitzungen der Stadtvertretung und ihrer Ausschüsse und welche Unterlagen erhält er, sofern er an Sitzungen teilnehmen darf? Darum ging es bei der Anfrage einer Stadtverwaltung.

Sitzungen der **Gemeindevertretung** sind grundsätzlich öffentlich, wenn nicht triftige Gründe, unter anderem berechnete Interessen einzelner, den Ausschluß der Öffentlichkeit verlangen. Insbesondere bei der Beratung von Personalangelegenheiten ist das durchweg der Fall.

Der Ausschluß der Öffentlichkeit bei Personalberatungen führt allerdings nicht zum Ausschluß des Personalrats. Das schleswig-holsteinische **Mitbestimmungsgesetz (MBG)** gewährt vielmehr dem zuständigen Personalratsmitglied bei mitbestimmungsrelevanten Maßnahmen ein Teilnahmerecht.

Dabei ist folgendes zu beachten:

- Der teilnehmende Personalrat muß für die betroffene Organisationseinheit (z.B. allgemeine Verwaltung, Stadtwerke, Krankenhaus) zuständig sein.
- Die Beratung muß einen Gegenstand betreffen, der dem Mitbestimmungsrecht unterliegt. Eine Teilnahme bei anderen vertraulichen Beratungsgegenständen wie Abgabensachen oder Grundstücksangelegenheiten kommt nicht in Betracht.
- Der Personalrat muß durch das den Vorsitz führende Mitglied bzw. durch den Gruppenvertreter vertreten sein.

Für nichtöffentliche **Ausschußsitzungen** gilt dieses Teilnahmerecht sinngemäß. Auch wenn die Öffentlichkeit im Einzelfall ausgeschlossen wird, bleibt ein Teilnahmeanspruch in Mitbestimmungsangelegenheiten bestehen, der durch den Beschluß nicht aufgehoben werden kann.

Der Personalrat hat weiter einen Anspruch auf **ausreichende Unterrichtung**. Grundsätzlich muß er im Rahmen seiner Aufgaben den gleichen Informationsstand erhalten, über den die Verwaltung bei der Vorbereitung ihrer Entscheidungen ver-

fügt. Dieser Anspruch richtet sich gegen die Stelle, bei der der Personalrat gebildet ist.

Soweit sein Teilnahmerecht an Sitzungen reicht, hat er auch einen Anspruch auf die **Sitzungsunterlagen**. In diesem Umfang sind ihm zur Sitzungsvorbereitung auch die Ausführungen in Rechnungsprüfungsberichten, ggf. in Auszügen, zur Verfügung zu stellen. Dabei kann es durchaus bereits vor einer Beratung in den Gremien erforderlich sein, daß ihm die Verwaltung vorliegende Berichte oder Auszüge zur Verfügung stellt, um der Unterrichtungspflicht frühzeitig nachzukommen. In welchem Umfang diese Verpflichtung besteht, muß im Einzelfall geprüft werden. Allerdings dürfen Personalakten nach dem Mitbestimmungsgesetz nur mit Einwilligung des Betroffenen eingesehen werden.

4.1.1.2 Teilnahme der Schwerbehindertenvertretung an den Sitzungen des Präsidialrates eines Gerichtes

Vertreter der Schwerbehinderten nehmen auch dann zu Recht an Sitzungen des Präsidialrats eines Gerichts teil, wenn personenbezogene Angelegenheiten ohne Beziehung zu Behindertenfragen besprochen werden.

Teilnahmerechte an Sitzungen waren auch Gegenstand einer Anfrage aus einem schleswig-holsteinischen Gericht. Die Vertretung der Schwerbehinderten nahm nach dem **Schwerbehindertengesetz** (SchwbG) an Sitzungen des **Präsidialrates** dieses Gerichtes auch dann teil, wenn Belange der Schwerbehinderten durch die Beratung nicht berührt wurden. Die Frage wurde gestellt, ob nicht vor dem Hintergrund des neuen Datenschutzrechts eine Beschränkung auf solche Sitzungsgegenstände geboten sei, durch die Schwerbehinderte betroffen würden.

Wir mußten darauf hinweisen, daß das SchwbG als **Spezialvorschrift** in diesem Punkt den allgemeinen Regelungen des LDSG vorgeht. Das SchwbG läßt die unbeschränkte Teilnahme der Schwerbehindertenvertretung an allen Sitzungen des Präsidialrates zu. Dieser vorrangigen Vorschrift muß entsprochen werden. Die Beteiligung an Verfahren ohne Schwerbehindertenbezug wird in Kauf genommen, um der Vertretung die eigene Entscheidung zu ermöglichen, in welchem Umfang die Interessen der Schwerbehinderten wahrzunehmen sind.

4.1.1.3 Wofür ein öffentlich Bediensteter einstehen muß

Das informationelle Selbstbestimmungsrecht von Mitarbeitern des öffentlichen Dienstes hindert nicht daran, ihre Amtsführung öffentlich zu erörtern. Erst wenn dienstrechtliche Bewertungen einfließen oder das Dienstverhältnis unmittelbar berührt wird, muß Vertraulichkeit gewährleistet sein.

Durch unkorrekte Buchungen in den Jahren 1987 bis 1990 ist es im Kur- und Badebetrieb einer Gemeinde zu erheblichen Verlusten gekommen. Zur Aufklärung dieser Verluste und zur Feststellung, ob und gegebenenfalls in welchem Umfang die Gemeinde gegen geltende Rechtsvorschriften verstoßen hat, wurde eine **Sonderprüfung** durch das **Gemeindeprüfungsamt** vorgenommen. Auf Beschluß der Gemeindevertretung sollte der daraufhin erstellte **Prüfungsbericht** zur Unterrichtung der Einwohner über mögliche Mißstände in der Verwaltung veröffentlicht werden. Als gesetzliche Grundlage hierfür wurde die Gemeindeordnung herangezogen, wonach die Gemeinde die Einwohnerinnen und Einwohner über allgemein bedeutsame Angelegenheiten der örtlichen Gemeinschaft zu unterrichten hat. Fraglich war, ob durch diese Veröffentlichung in unzulässiger Weise in die Persönlichkeitsrechte der Mitarbeiter eingegriffen würde.

Der Sonderprüfungsbericht enthielt für Teilbereiche der Verwaltung Aussagen über die Rechtmäßigkeit des Verwaltungshandelns der Gemeinde als Körperschaft des öffentlichen Rechts. Soweit handelnde Personen direkt angesprochen wurden, waren diese nicht in ihrer Eigenschaft als Privatpersonen tätig geworden, sondern hatten vielmehr als **Funktionsträger** öffentliche Aufgaben für ihren Rechtsträger wahrgenommen.

Der Übergang in den durch das Landesdatenschutzgesetz geschützten Persönlichkeitsbereich der Betroffenen findet aber regelmäßig erst dann statt, wenn sie als Mitarbeiter in ihrem **Rechtsverhältnis zum Dienstherrn** berührt werden. Dieser Fall dürfte in erster Linie bei einer Diskussion über die besonders geschützten Personalaktendaten eintreten.

Aber auch, wenn über eine bloße Darstellung der behördlichen Tätigkeit hinaus die dienstrechtliche Bewertung eines persönlich zurechenbaren fehlerhaften Verwaltungshandelns erfolgt (z.B. im Rahmen eines **Disziplinarverfahrens**), ist der Mitarbeiter als Privatperson angesprochen, die Datenschutzrechte für sich in Anspruch nehmen kann.

Der betreffende Sonderprüfungsbericht enthielt bis auf eine kleine Ausnahme keine Angaben, die über die Prüfung der Rechtmäßigkeit des Verwaltungshandelns der Gemeinde hinausgingen. Dabei lag es in der Natur der Sache, daß die einzelnen Maßnahmen der Verwaltung selbstverständlich auch natürlichen Personen zugeordnet werden konnten. Dies muß jedoch von Betroffenen, soweit sie öffentliche Aufgaben wahrnehmen, als Ausfluß des Dienstverhältnisses hingenommen werden. Eine Veröffentlichung von Verwaltungsentscheidungen wäre sonst generell nicht mehr möglich.

Die Behörde kann allenfalls versuchen, die mögliche Belastung für die Betroffenen dadurch zu mildern, daß Namen in dem Prüfungsbericht geschwärzt und nur noch die jeweiligen Funktionen angesprochen werden.

4.1.1.4 Führung von Personalakten über Referendare verbesserungsbedürftig

Die Personalaktenverwaltung hat bei Rechtsreferendaren grundsätzlich den gleichen Regeln zu folgen, wie die allgemeine Personalaktenverwaltung im öffentlichen Dienst. Das Ausbildungsmonopol des Staates muß jedoch zu einer Beschränkung der Bewerbungsunterlagen führen.

In diesem Jahr haben wir unsere Prüfungen im Personalverwaltungsbereich fortgesetzt. Ein besonderes Augenmerk richtete sich vor allem auf die Beschäftigten im **juristischen Vorbereitungsdienst**, da hier aufgrund des Ausbildungsmonopols des Staates für die Betroffenen kaum eine Wahlmöglichkeit besteht. Die Nichtzulassung eines Referendars zum juristischen Vorbereitungsdienst kommt faktisch einem Berufsverbot gleich.

Die beim Oberlandesgericht vorgefundenen Fehler zeigen einmal mehr, daß einheitliche Vorgaben zur Personaldatenverarbeitung im gesamten Landesbereich notwendig sind. Der Staatskanzlei, wie auch dem Innenminister, fällt hier eine besondere Verantwortung zu.

Neben bereits bei anderen Prüfungen festgestellten Mängeln (vgl. 13. TB, S. 17; 14. TB, S. 13) sind aber auch **neue Fehler** zutage getreten, die wegen ihrer grundsätzlichen Bedeutung besondere Erwähnung verdienen.

Bewerbungsverfahren

Die Verarbeitung von Bewerberdaten stellt einen Eingriff in die Rechte der Betroffenen dar, der ohne eine ausreichende Ermächtigungsgrundlage unzulässig ist. Bei Rechtsreferendaren ergibt sich die Rechtsgrundlage aus der Einwilligung des Bewerbers in Verbindung mit der „Verordnung über die Beschränkung der Einstellung in den juristischen Vorbereitungsdienst“, die enumerativ aufzählt, welche **Bewerbungsunterlagen** einzureichen sind.

Anders als bei üblichen Bewerbungssituationen muß hier beachtet werden, daß das Durchlaufen des Vorbereitungsdienstes Voraussetzung für den Abschluß der juristischen Ausbildung ist und daß der Staat das **Monopol der Juristenausbildung** hat. Einerseits ist daher der Rechtskandidat gezwungen, das Referendarverhältnis einzugehen, will er nicht seine juristische Ausbildung abbrechen, andererseits ist das Land verpflichtet (von hier nicht zu berücksichtigenden Ausnahmen abgesehen), jeden erfolgreich geprüften Rechtskandidaten auf seine Bewerbung hin in das Referendarverhältnis zu übernehmen. Im Gegensatz zu üblichen Bewerbungsverfahren können daher Bewerbungsunterlagen nur insoweit für die **Auswahlentscheidung** verwendet werden, als sie den Nachweis über die Voraussetzungen für die Einstellung enthalten. Nur diese Unterlagen sind für das Bewerbungsverfahren überhaupt erforderlich.

Tatsächlich werden aber auf der Grundlage der genannten **Verordnung** eine Reihe von Bewerbungsunterlagen verlangt, die für die Entscheidung **überflüssig** sind. Die Verordnung dürfte insoweit dem Grundsatz der Verhältnismäßigkeit nicht entsprechen.

Im einzelnen geht es dabei um folgende Unterlagen:

- zwei Lichtbilder
- ein Lebenslauf
- ein Führungszeugnis
- eine Erklärung für die Zahlung der Anwärterbezüge

Da eine Personalauslese wegen der bereits geschilderten besonderen Situation nicht stattfindet und die Daten über den beruflichen Werdegang schon im Personalbogen erfragt werden, beschränkt sich die tatsächliche Verwendung des **Lebenslaufes** bei der Einstellung durchweg darauf, daß er in der Personalakte **abgeheftet** wird. Ein aktuelles Führungszeugnis ist bei den meisten Bewerbern bereits vorhanden, da es schon für die Ablegung des ersten Staatsexamens vorgelegt werden muß und die Prüfungsakte im Bewerbungsverfahren beigezogen wird. Die für die Zahlung der Anwärterbezüge erforderlichen Daten dürfen erst nach Einstellungsentscheidung vom Landesbesoldungsamt erhoben werden. Es ist nicht vertretbar, wenn von der Abgabe der geforderten Erklärung die Berücksichtigung der Bewerbung als solcher **abhängig** gemacht wird. Die Verordnung sollte in diesem Sinne überarbeitet werden.

Die Prüfung hat darüber hinaus ergeben, daß die neuen bereichsspezifischen Vorschriften im Landesdatenschutzgesetz zur Verarbeitung von Personaldaten noch nicht hinreichend Beachtung gefunden haben. So wurden zum Beispiel Unterlagen über **zurückgezogene Bewerbungen** noch drei Jahre aufbewahrt, obwohl das Landesdatenschutzgesetz seit dem 01.01.1992 grundsätzlich eine Löschung verlangt, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt.

Führung von Personalakten

Es zeigten sich vor allem Probleme bei der **Einsichtnahme in Referendarpersonalakten**. Schon nach dem bisherigen Datenschutzrecht stand die Nutzung vollständiger Personalakten unter der Beschränkung des Erforderlichkeitsgrundsatzes. Mit den jüngsten Änderungen des Beamtenrechtsrahmengesetzes ist nun ausdrücklich klargelegt, daß Zugang zu Personalakten nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalakten beauftragt sind und nur **soweit** dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft **erforderlich** ist. Eine Vorlage von Personalakten bei anderen Stellen darf nicht erfolgen, soweit eine Auskunft ausreicht.

Der Zugang zu den vollständigen Personalakten der Referendare war nicht genügend beschränkt. So wurden diese Akten auf Anforderung dem gemeinsamen Prüfungsamt in Hamburg,

den unmittelbaren Dienst- und Fachvorgesetzten oder auch den einzelnen Ausbildungsbehörden (z.B. in der Kommunalstation), zur Verfügung gestellt.

Nach Beendigung des Vorbereitungsdienstes werden nach einer „Verfügung des Oberlandesgerichtspräsidenten über die Ausbildung der Juristen“ die beim Oberlandesgericht geführten Personalakten an den Justizminister abgegeben.

Da nach der **Juristenausbildungsordnung** der Präsident des Oberlandesgerichts die Referendarausbildung leitet, ist er bezüglich der Referendarakten die datenverarbeitende Stelle, auch wenn oberste Dienst- und Dienstaufsichtsbehörde der Justizminister ist.

Die Abgabe der Personalakten an den Justizminister stellt eine **Datenübermittlung** an eine andere Stelle dar, deren Zulässigkeit allein auf eine Verfügung gestützt wird, die keinen Rechtsnormcharakter hat. Nach unserer Auffassung muß diese Aktenabgabe mit Rücksicht auf das informationelle Selbstbestimmungsrecht der Referendare durch eine Rechtsnorm geregelt werden, wenn sie denn aus sachlichen Gründen für erforderlich gehalten wird.

Datensicherheit

Personalakten sind vor dem **Zugriff Unbefugter** hinreichend zu schützen. Dieser Grundsatz gilt auch für die Personalakten der Referendare. Zu verlangen ist nicht, daß die zu treffenden Sicherungsmaßnahmen einen mit physischer Gewalt vorgetragenen Angriff abwehren können. Es sollte aber zumindest ein unbemerkter Zugriff Dritter ausgeschlossen werden können.

Die Notwendigkeit, Personalakten hinreichend zu sichern, ist von der geprüften Stelle grundsätzlich erkannt worden. Es fehlte jedoch ein in sich **schlüssiges Gesamtkonzept**. So wurde für die Registratur ein Sicherheitsschloß angeschafft und darauf geachtet, daß dieser Raum ständig unter Verschuß gehalten wird. Auf die Anschaffung von Sicherheitsschlössern für die Sachbearbeiterbüros oder deren Verschuß bei Abwesenheit der Mitarbeiter wurde dagegen verzichtet, obwohl sich auch in diesen Räumen ständig Personalakten befinden.

Völlig inakzeptabel war die praktizierte Aktenverteilung in **offenen Regalen** auf dem Flur. In diesen Regalen befanden sich während der Prüfung, trotz erheblichen Publikumsverkehrs, völlig unbeaufsichtigt Personalakten, die für jedermann frei und unkontrolliert zugänglich waren. Dies war als eine erhebliche Gefährdung der Rechte der Betroffenen zu beanstanden.

4.1.1.5 Kultusministerin reagiert auf Prüfbericht

Die bisherigen Reaktionen auf die Kontrolle der Verarbeitung von Personaldaten der Lehrer sind nicht ausreichend. Weitere rasche Änderungen der bisherigen Praxis sind, auch im Hinblick auf eingetretene Änderungen im Datenschutz- und im Beamtenrecht, notwendig.

In unserem 13. Tätigkeitsbericht (S. 11) haben wir ausführlich über Prüfungen im Personalverwaltungsbereich für Lehrer berichtet. In einer vor kurzem vorgelegten **ersten Stellungnahme** hat das Kultusministerium zugesagt, sowohl für die Datenerhebung im Bewerbungsverfahren als auch für die Führung von Personalakten auf der Grundlage der Prüfungsfeststellungen **neue Konzepte und Vorgaben** zu erarbeiten. Für die Personalaktenführung liegt bereits ein erster Richtlinienentwurf vor, der allerdings in wichtigen Teilbereichen keine bzw. unzureichende Festlegungen enthält. Auch die Stellungnahme selbst läßt es in vielen Punkten offen, ob und in welchem Umfang die Auffassungen des Kultusministeriums tatsächlich mit denen des Landesbeauftragten übereinstimmen.

Ein Teilerfolg konnte inzwischen bei der **Übermittlung** von **Personalakten** an Dritte erzielt werden (14. TB, S. 15). In Absprache mit der Finanzministerin und dem **Landesbesoldungsamt** wurde ein Verfahren eingeführt, durch das gewährleistet wird, daß die personalverwaltenden Stellen dem Landesbesoldungsamt nur noch die im Einzelfall zur Aufgabenerfüllung tatsächlich erforderlichen Personaldaten übermitteln. Vollständige Personalakten der Mitarbeiter dürfen generell nur noch mit schriftlicher Einwilligung der Betroffenen weitergegeben werden.

4.1.2 Verfassungsschutz

Datenbestände werden bereinigt

Die Verfassungsschutzbehörde bereinigt ihre Datensammlungen. Bis zum Jahresende sollen alle Daten gelöscht sein, die mit dem neuen Verfassungsschutzgesetz nicht mehr in Einklang stehen.

Nachdem 1991 das neue Landesverfassungsschutzgesetz mit wesentlichen Änderungen der für die Datenverarbeitung relevanten Bestimmungen in Kraft getreten ist, hat der Innenminister als Behörde für Verfassungsschutz unter unserer Beratung im Berichtsjahr ein Konzept zur Bereinigung der Datenbestände erarbeitet. Derzeit ist man dabei, die Datensammlungen nach Maßgabe dieses Konzepts zu bereinigen. Mit einem Abschluß der Lösch- und Bereinigungsarbeiten ist bis Ende 1993 zu rechnen. Es ist zu erwarten, daß die Datenbestände sowohl in Akten und Karteien als auch in automatisierten Datensammlungen nach Beendigung der Aktion einen deutlich geringeren Umfang haben.

4.1.3 Öffentliche Sicherheit

4.1.3.1 Das neue Landesverwaltungsgesetz

Das neue Polizeigesetz setzt der polizeilichen Datenverarbeitung rechtsstaatliche Grenzen. Seine Auswirkungen können aus der Perspektive seltener Einzelfälle nicht seriös beurteilt werden.

Im Berichtsjahr ist das neue schleswig-holsteinische Landesverwaltungs-gesetz in Kraft getreten, das im Bereich des Polizeirechts die **Konsequenzen** aus dem **Volkszählungsurteil** des Bundesverfassungsgerichts zieht. Über Einzelheiten der Neuerungen wurde im 14. TB (S. 22) berichtet.

Bislang konnten noch keine umfassenden Erfahrungen mit seiner Anwendung gewonnen werden. In einer ersten **Querschnittsauswertung** sind wir der Frage nachgegangen, ob die neu in das Gesetz aufgenommene **zweijährige Wiedervorlagefrist** für Erstspeicherungen beachtet wird. Dabei haben sich keine Gründe zur Beanstandung ergeben.

Erstaunlich schnell waren Stimmen zu vernehmen, das Gesetz müsse **novelliert** werden. Während etwa die Konsequenzen aus der datenschutzrechtlichen Kontrolle des Jahres 1988 in wichtigen Teilen noch nicht gezogen sind (vgl. Tz. 4.1.3.2), wurde schon wenige Monate nach Inkrafttreten des neuen Gesetzes Klage über diese oder jene – angeblich zu restriktive – Bestimmung geführt. Von Behinderungen und Einengungen polizeilicher Spielräume war die Rede. Das muß nicht gegen das Gesetz sprechen. Sinn jeder polizeirechtlichen Regelung ist es, die polizeilichen Handlungsmöglichkeiten **rechtsstaatlich** zu definieren. Gelegentlich werden in der Diskussion **skurrile Einzelfälle** vorgebracht, in denen unzuträgliche Auswirkungen aufgetreten seien. Dabei wird aber übersehen, daß die Tauglichkeit einer Vorschrift seriös nicht aus dem Blickwinkel des extremen Sonderfalls, sondern nur im Hinblick auf die „normale“ tägliche Anwendung beurteilt werden kann. So gesehen ist einer sachbezogenen Diskussion mit dem Herausstellen und Propagieren extremer Einzelfälle wenig gedient.

Novellierungsbedarf sah der Gesetzgeber allerdings, weil zwei Richter eines Gerichts bei der richterlichen Genehmigung verdeckter polizeilicher Datenerhebungsmaßnahmen den Standpunkt vertraten, der Betroffene müsse von Verfassungs wegen vor der richterlichen Entscheidung **rechtliches Gehör** erhalten. Wenn dies zuträfe, dann wäre auch jegliche richterliche Genehmigung von Hausdurchsuchungen und Telefonabhörmaßnahmen rechtswidrig, wenn sie ohne vorherige Anhörung des Betroffenen ergeht. Täglich würden dann in Deutschland dutzendfach empfindliche Rechtseingriffe unter Verstoß gegen die Verfassung begangen. Es ist aber allgemein anerkannt, vom Bundesverfassungsgericht bekräftigt und im übrigen tägliche Praxis, daß bestimmte Ermittlungsmaßnahmen ohne Kenntnis des Betroffenen vorgenommen werden. In diesen Fällen hat **nach Abschluß** der Maßnahme die **Unterrichtung** zu erfolgen, damit zumindest im nachhinein Rechtsschutz erlangt werden kann.

Genau dies war bereits im Polizeigesetz geregelt. Daß nunmehr ausdrücklich in das Gesetz der Zusatz aufgenommen werden soll, daß der Betroffene vor der gerichtlichen Entscheidung kein rechtliches Gehör erhält, dient der Klarstellung.

4.1.3.2 Konsequenzen aus der Datenschutzprüfung bei der Polizei weiterhin unbefriedigend

Die Konsequenzen aus der datenschutzrechtlichen Kontrolle bei der Polizei kommen nicht im notwendigen Tempo voran. Zwar ist die Zahl der Kriminalakten noch einmal von 240.000 auf 160.000 verringert worden. Aber auch mehr als drei Jahre nach Abschluß der Prüfung sind wichtige Zusagen des Innenministers noch nicht realisiert.

Über die Querschnittskontrolle der Datenverarbeitung bei den Polizeibehörden ist nunmehr zum dritten Mal zu berichten (vgl. 14. TB, S. 24). Allerdings kann nach wie vor nicht der Abschluß der Umsetzungsmaßnahmen vermeldet werden. Auch im vergangenen Jahr ist es dem Innenminister **nicht gelungen**, die **notwendigen Konsequenzen** aus dieser Kontrolle abschließend zu ziehen. Zwar ist anzuerkennen, daß die **Kriminalaktenbestände** beim Kriminalpolizeiamt **spürbar bereinigt** worden sind. Waren zum Zeitpunkt der Kontrolle noch 240.000 Kriminalakten gespeichert, so ging die Zahl zum Ende des Berichtsjahres auf ca. 160.000 zurück. Dies ist eine erfreuliche Entwicklung. Bei näherem Zusehen zeigt sich, daß offenbar in erster Linie Bagatellfälle bereinigt wurden und sich die Herabsetzung der Regelspeicherfrist von 10 auf 5 Jahre deutlich bemerkbar macht. Es bleiben aber eine Reihe von gravierenden Punkten offen. Im einzelnen geht es noch um folgendes:

Kriterien für die Anlegung von Kriminalakten

Wir hatten u.a. kritisiert, daß bei der **Anlegung von Kriminalakten** häufig schematisch verfahren wird, so daß auch in Bagatellfällen Kriminalakten gespeichert werden. Auch der Innenminister räumte in seiner ersten Stellungnahme von Anfang 1991 hier einen Regelungsbedarf ein. Unter anderem hielt er eine Präzisierung der Voraussetzungen für das Anlegen einer Kriminalakte für notwendig, einschließlich einer Aufzählung von Standardfällen, bei denen in der Regel keine Akte angelegt wird. Für besonders gelagerte Fälle sollten besondere Entscheidungsvorbehalte (z.B. durch den Dienststellenleiter) vorgesehen werden. Anfang 1992 teilte der Innenminister mit, es sei eine **Arbeitsgruppe beim Kriminalpolizeiamt** zur Überarbeitung der Regelungen für die Führung von Kriminalakten eingerichtet worden. Die vom Landesbeauftragten in diesem Zusammenhang geltend gemachten Mängel bei der Anlegung von Kriminalakten würden von dieser Arbeitsgruppe berücksichtigt.

Über **Ergebnisse** ist uns bis zur Erstellung dieses Berichts **nichts bekannt** geworden.

Die Notwendigkeit, nunmehr umgehend zu untergesetzlichen Regelungen über die Anlegung und Führung von Kriminalakten zu kommen, ergibt sich auch daraus, daß Mitte des Jahres das Landesverwaltungsgesetz in Kraft getreten ist. Es sieht für

Bagatelldelikte Einschränkungen bei der Datenverarbeitung vor. Gerade auch im Hinblick auf gelegentlich vorgebrachte Klagen, das neue Polizeirecht sei zu kompliziert und bedürfe der Auslegungshilfe für die Praxis, wäre es notwendig, möglichst umgehend zu einer gut handhabbaren **Verwaltungsvorschrift** zu kommen. In ihr sollten sowohl die in unserem Prüfbericht aufgeführten datenschutzrechtlichen Mängel der bisherigen Praxis als auch die neuen Regelungen im Landesverwaltungsgesetz berücksichtigt werden.

Das Kriminalpolizeiamt hat hierzu kurz vor Fertigstellung dieses Berichtes ergänzend mitgeteilt, die für die Anlegung von Kriminalakten zuständigen Mitarbeiterinnen und Mitarbeiter seien im Hinblick auf das neue Polizeirecht besonders geschult worden. Sie seien zu den notwendigen Entscheidungen, ggf. abweichend von den noch bestehenden alten Richtlinien, in der Lage. Dies kann allerdings nach unserer Auffassung den Erlaß der Verwaltungsanweisung nicht ersetzen.

Kennzeichnung der Personengruppen in der PED

Ein anderer Kritikpunkt in unserem Prüfbericht war, daß man in der polizeilichen Erkenntnisdatei PED nicht unterscheiden kann, ob eine Person als „**Beschuldigter**“, „**Verdächtiger**“, „**Zeuge**“ oder „**andere Person**“ gespeichert ist. Da auf die Daten der PED alle Polizeidienststellen des Landes unmittelbar Zugriff haben, also auch solche Dienststellen, die selbst nicht die zugehörigen Kriminalakten führen, kommt es entscheidend darauf an, daß man bereits dem Datensatz entnehmen kann, in welcher Beziehung die betreffende Person zum jeweiligen Straftatvorwurf steht.

Diese Forderung leuchtete zunächst auch dem Innenminister ein. In einer ersten Stellungnahme teilte er mit, Anfang 1992 sei mit einer Verfahrensänderung zu rechnen. In einer weiteren, späteren Stellungnahme, wurde dies wieder zurückgenommen, da es **finanziell unangemessen** aufwendig sei und „zu Problemen im INPOL-Verbund“ führen würde. Nunmehr ist zu diesen Fragen aber auch das **neue Landesverwaltungsgesetz** zu berücksichtigen. Dort sind Sonderregelungen für die Verarbeitung und Verwendung von Daten über Zeugen, Hinweisgeber und sonstige Auskunftspersonen vorgesehen. Unter anderem muß die weitere Notwendigkeit der Speicherung derartiger Daten jährlich überprüft werden. Außerdem ist vorgeschrieben, daß Daten über diese Personen nur an andere Polizeibehörden, nicht aber an sonstige Behörden und öffentliche Stellen übermittelt werden dürfen. Auch daraus dürfte sich die Notwendigkeit ergeben, derartige Daten besonders zu kennzeichnen, damit die gesetzlichen Pflichten erfüllt werden können. Wir halten es deshalb nach wie vor für notwendig, **Personendatensätze** in der PED entsprechend zu **klassifizieren**.

Überarbeitung des PED-Handbuches

Das sogenannte **PED-Handbuch** regelt zwar die technische Handhabung dieses Dateiverfahrens im Detail, sagt aber nichts über die rechtliche Zulässigkeit der Speicherung von Daten in der PED aus. In einer ersten Stellungnahme Anfang 1991 sagte der Innenminister zu, das PED-Handbuch umgehend ändern zu wollen, damit den Kritikpunkten Rechnung getragen werden könne. Bislang ist uns noch keine geänderte Fassung des PED-Handbuches zugegangen.

Besonderer Zugriffsschutz für Daten über Polizeibeamte

Da die in der PED gespeicherten Informationen grundsätzlich dem Zugriff jedes Polizeibeamten unterliegen, hatten wir vorgeschlagen, für die dort über Polizeibeamte gespeicherten personenbezogenen Daten einen **besonderen Zugriffsschutz** vorzusehen. Nachdem zunächst mitgeteilt worden war, es werde ein Verfahren realisiert, das den Zugriff auf Datensätze von Polizeibeamten nur über eine besondere Berechtigung zuläßt, hat der Innenminister jetzt eingewandt, die vorgesehene Lösung sei zu kostenaufwendig. Es werde deshalb nunmehr angestrebt, Polizeibeamte betreffende Datensätze so zu reduzieren, daß ohne zusätzliche Information aus der Kriminalakte eine eindeutige Identifizierung der betreffenden Person nicht möglich sei. Für uns stellt sich dabei allerdings die Frage, welchen Sinn die Speicherung dieser Daten in der PED dann noch macht, wenn sie tatsächlich vollständig anonymisiert sein sollten.

Vorgangsverwaltung

Ein weiterer Vorschlag im Prüfbericht ging dahin, für die sogenannte **Vorgangsverwaltung** der Polizei Verwaltungsvorschriften zu erlassen, in denen Festlegungen getroffen werden über

- die Art der Führung der Vorgangsablagen,
- deren Verhältnis zu den kriminalpolizeilichen Sammlungen,
- die zulässigen Zugriffs- und Nutzungsmöglichkeiten,
- die Speicherdauer und
- die Sicherung der Datenbestände.

Zunächst hatte der Innenminister angekündigt, die entsprechende Regelung solle Anfang 1992 in Kraft treten und werde dem Landesbeauftragten demnächst zur Mitzeichnung vorgelegt. Dies ist bislang nicht erfolgt. Nunmehr schreibt auch das Landesverwaltungsgesetz verbindlich vor, daß der Innenminister Mittel und Umfang der Vorgangsverwaltung durch Verwaltungsvorschrift im Benehmen mit dem Landesbeauftragten für den Datenschutz zu bestimmen hat.

Erkennungsdienstliche Maßnahmen

Umstritten war zunächst unsere Forderung, die Gründe für **erkennungsdienstliche Maßnahmen** in jedem Einzelfall auf dem Erhebungsbogen zu **dokumentieren**. Dies erscheint notwendig, weil die rechtlichen Voraussetzungen für ererkennungsdienstliche Maßnahmen nach der Strafprozeßordnung und nach dem neuen Landesverwaltungsgesetz erheblich voneinander abweichen.

Nachdem zunächst in den Gesprächen mit dem Innenminister keine Übereinstimmung über die Notwendigkeit derartiger ergänzender Hinweise auf dem Erhebungsbogen zu erzielen war, hat er nunmehr mitgeteilt, es sei ein neuer Vordruck entwickelt worden, der mit dem Landesbeauftragten abgestimmt werden solle. Bis zur Fertigstellung dieses Berichts lag der Entwurf noch nicht vor.

Damit im Zusammenhang steht die weitere Forderung, die **Richtlinien für ererkennungsdienstliche Behandlungen** (sogenannte ED-Richtlinien) zu überarbeiten. Nachdem zunächst umstritten war, ob es einer Überarbeitung der ED-Richtlinien überhaupt bedarf, teilte der Innenminister nunmehr mit, hierzu sei noch die Abstimmung mit dem Justizminister notwendig.

Datenverarbeitung beim Staatsschutz

Der Prüfbericht befaßte sich auch mit der Datenverarbeitung im Bereich des **polizeilichen Staatsschutzes**. Unter anderem wurde kritisiert, daß in den dortigen Dateien für „äußere Sicherheit“ und „innere Sicherheit“ über die Strafverfolgung und Gefahrenabwehr im eigentlichen Sinne hinaus auch sogenannte **„Vorfelddaten“** gespeichert werden. Außerdem war verlangt worden, beide Dateien zu bereinigen.

Der Innenminister hat zwischenzeitlich mitgeteilt, daß die Datei „äußere Sicherheit“ bereinigt wurde und daß Regelungen für die künftige Datenerfassung in dieser Sammlung in Vorbereitung seien. Auf dem Gebiet der Datei „innere Sicherheit“ sei eine Bereinigung bislang noch nicht erfolgt. Neue Weisungen für die Führung dieser Sammlung befänden sich in Vorbereitung. Auch im Hinblick auf die neuen Vorschriften des Landesverwaltungsgesetzes sei eine Änderung und Neufassung der bestehenden Ausführungsbestimmungen notwendig. Es liege bereits ein Entwurf vor, der Anfang 1993 mit dem Landesbeauftragten abgestimmt werden solle.

Berücksichtigung von Freisprüchen

In verschiedenen Zusammenhängen war im Prüfbericht die Tatsache kritisiert worden, daß die Polizei in vielen Fällen nichts über den **Ausgang des justitiellen Verfahrens** weiß. Aus diesem Grunde enden zahlreiche Kriminalakten mit der Abgabe der Sache an die Staatsanwaltschaft, ohne daß nachgetragen würde, wie die Justiz den Sachverhalt endgültig be-

urteilt hat. Die Gründe hierfür lagen in der Vergangenheit in erster Linie in der **fehlenden Rückmeldung** der Staatsanwaltschaft an die Polizei, aber auch in Defiziten bei der Umsetzung der von der Justiz gemeldeten Verfahrensausgänge.

Hierzu sind nunmehr zwei Änderungen eingetreten. Zum einen verlangt das Landesverwaltungsgesetz, daß die Polizei sich aktiv, spätestens nach zwei Jahren, bei der Justiz nach dem Ausgang des Verfahrens erkundigt. Zum anderen hat der Innenminister einen Realisierungsvorschlag für einen **automatisierten Abgleich** zwischen der polizeilichen Erkenntnisdatei **PED** und der Geschäftsstellenautomation der Staatsanwaltschaften (**GAST-SH**) vorgelegt. Demnach ist beabsichtigt, die Daten über den Ausgang des justitiellen Verfahrens zwischen PED und GAST automatisiert auszutauschen. Hiergegen werden von uns im Grundsatz keine Einwände erhoben. Wir haben aber darauf aufmerksam gemacht, daß die Meldung des Ausgangs des gerichtlichen Verfahrens an die Polizei das Problem nur zum Teil löst.

Es kommt ergänzend darauf an, daß die Polizei diese Information auch in ihren Datensammlungen **umsetzt**. Wir haben deshalb den Innenminister gebeten, zugleich mit der Realisierung des automatisierten Nachrichtenaustausches PED-GAST **Kriterien** zu entwickeln, die bei der Entscheidung über die weitere Speicherung in den polizeilichen Dateien zugrunde zu legen sind. Dabei wird insbesondere auch zu beachten sein, daß nach dem neuen Landesverwaltungsgesetz Daten zu löschen sind, wenn der dem Ermittlungsverfahren zugrunde liegende Verdacht entfallen oder wenn ein Verfahren nach § 153 Strafprozeßordnung eingestellt worden ist. Bis zur Erstellung dieses Berichts waren entsprechende Kriterien noch nicht entwickelt.

4.1.3.3 Neuregelung der Lichtbildvorzeigekartei

Aufbau und Führung der Lichtbildvorzeigekartei sind neu geregelt worden. Die datenschutzrechtlichen Kritikpunkte an der bisherigen Praxis sind überwiegend berücksichtigt. In einem wichtigen Punkt bleiben die neuen Richtlinien aber hinter den Erwartungen zurück.

Die Lichtbildvorzeigekarteien der Polizei sind deshalb **besonders sensible Datensammlungen**, weil sie nicht nur zum internen Gebrauch, sondern überwiegend zur **Vorlage gegenüber Dritten dienen**. Damit wird bei Zeugen und Opfern von Straftaten oder sonstigen Auskunftspersonen der Anschein erweckt, der Betreffende gehöre zum Kreis der potentiell Verdächtigen. Dies stellt eine erhebliche Belastung für den Betroffenen dar, die über die bloße Aufbewahrung erkennungsdienstlicher Unterlagen weit hinausgeht.

Daher hatten wir nach unserer Querschnittskontrolle bei der Polizei 1989 unter anderem gefordert, die Vorschriften für die Lichtbildvorzeigekartei zu überarbeiten, damit z. B. der Aus-

gang des Verfahrens vor Gericht bei der weiteren Aufbewahrung von Fotos in der Lichtbildvorzeigekartei berücksichtigt wird (s. 12. TB, S. 23). Wir hatten bei unserer Kontrolle Fälle gesehen, in denen trotz **Freispruchs** die Daten in der Lichtbildvorzeigekartei nicht gelöscht worden waren. Der Innenminister ist dieser Anregung mit der Neufassung der Richtlinien für die Durchführung von Wahllichtbildvorlagen und die Führung von Lichtbildvorzeigekarteien nunmehr gefolgt.

Die **Richtlinien verbessern** das bisherige Verfahren datenschutzrechtlich in einer Reihe von Punkten. So wurden die Voraussetzungen für die Speicherung von Fotos in der Lichtbildvorzeigekartei enger gefaßt. Nach Ausgang des gerichtlichen Verfahrens ist zu prüfen und gegebenenfalls zu dokumentieren, ob die Voraussetzungen für die Speicherung in der Lichtbildvorzeigekartei auch weiterhin vorliegen.

An einem – aus datenschutzrechtlicher Sicht gravierenden – Punkt wurde unsere Anregung jedoch nicht aufgegriffen. Die **Aufbewahrungsfristen** der Lichtbildvorzeigekartei sollten, gerade weil die Lichtbilder ständig dritten Personen gezeigt werden, kürzer als die für Kriminalakten sein. Statt dessen ist aber vorgesehen, daß sich die Aufbewahrungszeit nach wie vor nach der Aufbewahrung der Kriminalakte richten soll. Dies wird damit begründet, daß es sich bei den in die Lichtbildvorzeigekartei eingestellten Bildern um einen Teil der erkennungsdienstlichen Unterlagen handle. Sie hätten damit hinsichtlich der Aufbewahrung und Nutzung grundsätzlich denselben Voraussetzungen und Fristen zu unterliegen wie die Unterlagen insgesamt. Diese Begründung verfängt aber nicht, weil Kriminalakten – im Gegensatz zu den in der Lichtbildvorzeigekartei gespeicherten Fotos – nicht Dritten zur Einsichtnahme vorgelegt werden.

4.1.3.4 In den Mühlen der Sicherheitsbürokratie

Auch „harmlose“ Speicherungen bei Sicherheitsbehörden können für den Betroffenen unangenehme Folgen haben. Die enge Zusammenarbeit zwischen den Sicherheitsbehörden kann zur Weitergabe von Daten und damit letztlich dazu führen, daß sie dem Betroffenen an ganz anderer Stelle entgegengehalten werden.

Immer wieder ist das Argument zu hören: „Wer nichts zu verbergen hat, braucht Datenerhebung und Datenspeicherung bei den Sicherheitsbehörden nicht zu befürchten.“ So gesehen hätte ein Bundeswehrsoldat, der sich an uns wandte, beruhigt schlafen können. Gleichwohl wurde er vom Militärischen Abschirmdienst (MAD) im Rahmen einer routinemäßigen **Sicherheitsüberprüfung** mit der Frage überrascht, was er denn im August 1989 „mit der Polizei zu tun gehabt“ habe.

Er wußte es wirklich nicht und erhielt zur Antwort, er sei „im Zentralcomputer der Staatsanwaltschaft Kiel“ gespeichert. Delikt: Diebstahl, mehr könne man dazu nicht sagen.

Was war der Hintergrund? Es hatte ein Ermittlungsverfahren gegen den Petenten wegen Diebstahlsverdachts gegeben. Er sollte einer Bekannten geholfen haben, einen Schreibtisch im Wert von 100,- DM, der dieser nicht gehörte, aus einer Wohnung abzuholen und zu verkaufen. Das Verfahren wurde eingestellt, da sich die **Vorwürfe** als **haltlos** erwiesen. Der Vorgang wurde routinemäßig im Informationssystem GAST der Staatsanwaltschaft für fünf Jahre gespeichert.

Wie aber war der **MAD** an die Information gekommen? Der Ermittlungsakte war kein Nachweis über eine etwaige Datenübermittlung zu entnehmen. Der leitende Oberstaatsanwalt in Flensburg teilte mit, daß früher Mitarbeitern des MAD bei ihrem persönlichen Erscheinen **mündlich Auskunft** gegeben worden sei. Nach dem Inkrafttreten des neuen LDSG würden Auskünfte schriftlich dokumentiert.

Nachforschungen des Bundesbeauftragten für den Datenschutz, der im Hinblick auf seine Zuständigkeit für den MAD eingeschaltet worden war, ergaben, daß auch die **schleswig-holsteinische Polizei** beteiligt war. Sie erteilte dem MAD kurz und bündig die Auskunft: „Straftat: Diebstahl, Tatzeit ..., Geschäftszeichen der Staatsanwaltschaft ..., Ausgang des Verfahrens hier nicht bekannt.“

Daraufhin wurde seitens des MAD bei der örtlich zuständigen Staatsanwaltschaft in Flensburg nachgefragt und in Erfahrung gebracht, daß das Ermittlungsverfahren eingestellt worden ist. Die **näheren Umstände** und weswegen das Verfahren genau eingestellt worden ist, wurden offenbar weder erfragt noch mitgeteilt. Statt dessen wurde der Soldat mit der eingangs zitierten Frage überrascht. Hätte man sich bei der Staatsanwaltschaft ordnungsgemäß erkundigt, wäre ihm das peinliche Verhör erspart geblieben.

Es stellt sich außerdem die Frage, warum die Polizei dem MAD den **Straftatverdacht** mitteilte, obwohl sie über den Ausgang des Verfahrens nichts wußte. Das Kriminalpolizeiamt meinte dazu, dies sei erforderlich gewesen, weil es dem MAD im Rahmen der Sicherheitsüberprüfung gerade darauf ankomme und weil er nur so in der Lage sei, eine (notfalls auch sehr kurzfristige) Entscheidung darüber zu treffen, ob in der Person des Überprüften ein Sicherheitsrisiko besteht. Die Übermittlung des Aktenzeichens allein hätte diesem Bedürfnis nicht genügt.

Dies wiederum ist für uns nicht einleuchtend, denn wir halten es für kaum denkbar, daß auf der Basis einer Information etwa des Inhalts „Tatverdacht Diebstahl, Ausgang des Verfahrens unbekannt“, irgendeine Entscheidung getroffen werden kann, ohne die Akten der Staatsanwaltschaft einzusehen. Dazu ist aber eine **Vorabinformation** über einen **unbewiesenen Tatverdacht** nicht notwendig.

Das Ende der Geschichte? Die Polizei nahm den Briefwechsel mit uns zum Anlaß, ihrer **Nachberichtspflicht** nach dem neuen LDSG Genüge zu tun und teilte dem MAD mit, daß sich

der Anfangsverdacht gegen den Petenten nicht bestätigt habe. Sie bat den MAD, seine Unterlagen zu berichtigen. Wenn der Petent sich nichts zu Schulden kommen läßt, werden seine Daten bei Polizei und Staatsanwaltschaft nach fünf Jahren gelöscht. Solange er allerdings in sicherheitsempfindlicher Funktion im Bundeswehrbereich beschäftigt ist, bleibt seine **Sicherheitsüberprüfungsakte** beim MAD samt Anfangsverdacht und Berichtigung durch die Polizei erhalten.

4.1.3.5 Sensible Daten über die Familien von Ausreißern

In einer Spezialdatei werden Daten über Vermißte, unbekannte Tote, Ausreißer und unbekannte hilflose Personen gespeichert. Als vermutliche Gründe des Verschwindens werden auch Daten über die Familiensituation erfaßt.

Zu den vielen Dateien, die von den Polizeien der Länder und dem Bundeskriminalamt im Verbund betrieben werden, gehört seit Jahren die Datei „**Vermißte, unbekannte Tote, unbekannte hilflose Personen**“ (VERMI/UTOT). Im vergangenen Jahr ist die Errichtungsanordnung für diese Datei neu gefaßt worden. Gegen eine Datensammlung, die das Wiederauffinden vermißter Personen und die Identifizierung unbekannter Toter ermöglichen soll, gibt es im Grundsatz nichts einzuwenden. Auch das neue Landesverwaltungsgesetz enthält eine Rechtsgrundlage für die Speicherung derartiger Daten. Gleichwohl erhoben wir im Detail Bedenken gegen einige der vorgesehenen Datenfelder.

So erlaubt die Errichtungsanordnung die Speicherung **personegebundener Hinweise**, wie etwa „gewalttätig“, „Ausbrecher“, „Ansteckungsgefahr“, „geisteskrank“, „Betäubungsmittelkonsument“, „Freitodgefahr“, „Prostitution“. Es bestehen Bedenken, derartige, in erster Linie belastende Bewertungen über Personen zu speichern, die keiner Straftat verdächtig sind. Des weiteren sollen Daten über etwaige vorhandene erkennungsdienstliche Unterlagen erfaßt werden. Hierzu zählt auch ein Vermerk über die „**Art der ED-Maßnahme**“. Auf diese Weise ist es möglich, Informationen über den Verdacht möglicherweise früher begangener Straftaten in einer Datei zu speichern, die doch nur dem Wiederauffinden vermißter Personen und der Identifizierung von Toten dienen soll.

Erhebliche Bedenken waren schließlich noch gegen die Datengruppe „**vermutliche Motive**“ anzuführen, in der Gründe des Verschwindens Vermißter erfaßt werden können. Dort gibt es folgende Datenfelder: „Unglück“, „Familienzwistigkeiten“, „Trunksucht“, „Flucht vor Strafe“, „Wirtschaftliche Schwierigkeiten“, „Freitod“, „Hilflosigkeit“, „Abenteurer“, „Streuner“.

In unserer Stellungnahme an den Innenminister haben wir uns auf den Standpunkt gestellt, daß derartige Hinweise, die ja zum Teil nicht nur den Vermißten selbst, sondern auch seine **Familie** betreffen, unverhältnismäßig sind. Auf diesem Wege

können alle Polizeibehörden Informationen über mögliche Motive für das Verschwinden z.B. junger Ausreißer abfragen, ohne daß überzeugend dargelegt wäre, daß dies zur rechtmäßigen Aufgabenerfüllung erforderlich ist. Der Innenminister hat zunächst im Arbeitskreis II der Innenministerkonferenz der Errichtungsanordnung nicht zugestimmt, in der Innenministerkonferenz dann aber nicht mehr widersprochen.

4.1.3.6 Wozu das Paßfoto noch von Nutzen sein kann

Die Polizei darf im Rahmen ihrer Ermittlungen auch Fotos aus dem Paß- und Personalausweisregister nutzen. Bei Ermittlungen wegen Ordnungswidrigkeiten sollte eine Bagatellgrenze beachtet werden.

In einer Reihe von Eingaben machten Bürger ihrem Ärger über polizeiliche Ermittlungsmethoden Luft. Was war geschehen? Die Betroffenen standen im Verdacht, **Verkehrsordnungswidrigkeiten** begangen zu haben. Als die Polizei bei ihren Ermittlungen nicht weiter kam, weil sich die Verdächtigen auf ihr Zeugnisverweigerungsrecht beriefen, verglich sie die Beweisfotos mit den **Fotos im Paß- oder Personalausweisregister**. Auf diesem Wege konnten die Verdächtigen identifiziert werden.

Wir gingen den Fällen nach und prüften bei dieser Gelegenheit generell die Verfahrensweise in der betreffenden Polizeidirektion. Im Ergebnis war **nichts zu beanstanden**. Das Paß- und das Personalausweisgesetz sehen für die Polizei ausdrücklich die Befugnis vor, Fotos in diesen Registern auszuwerten. Die gesetzlichen Voraussetzungen hierfür sind nicht allzu eng, so daß Daten auf diesem Weg relativ einfach erhoben werden können. Im wesentlichen muß die Polizei im Rahmen ihrer Zuständigkeit handeln und ohne die Registerdaten nicht in der Lage sein, ihre Aufgaben zu erfüllen. Voraussetzung ist weiterhin, daß die Daten beim Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand erhoben werden können oder nach der Art der Aufgabenerfüllung von einer Erhebung beim Betroffenen abgesehen werden muß. Die ersuchende Stelle trägt die Verantwortung für das Vorliegen dieser Voraussetzungen. Ersuchen dürfen nur von besonders vom Behördenleiter dafür ermächtigten Mitarbeitern gestellt werden und sind aufzuzeichnen.

Diese **Voraussetzungen** waren in den geprüften Fällen **eingehalten**. Zu kritisieren war lediglich, daß in zwei Fällen die Fotos von Verdächtigen bereits Nachbarn zum Zwecke der Identifizierung gezeigt worden waren, statt direkt das Register auszuwerten. Im Ergebnis führt diese gesetzliche Situation dazu, daß die Polizei die **Fotos in Paß- und Personalausweisregistern** genau wie **erkennungsdienstliches Material** nutzen kann. So sehr wir die Empörung der Betroffenen verstehen konnten, so handelte die Polizei auf dem Boden – wenn auch weitgefaßter – gesetzlicher Ermächtigungen, die anlässlich der

Einführung maschinenlesbarer Ausweispapiere geschaffen worden waren.

Wir haben dem Innenminister vorgeschlagen, im Sinne des Verhältnismäßigkeitsprinzips die Einsichtnahme in Paß- und Personalausweisregister nur dann vornehmen zu lassen, wenn eine Ordnungswidrigkeit aufzuklären ist, die zumindest mit einem Bußgeld von 80,- DM oder der Eintragung in das Bußgeldregister bedroht ist. Ähnliche Regelungen bestehen auch in anderen Bundesländern.

4.1.4 Ausländerwesen

4.1.4.1 Neufassung des Asylverfahrensgesetzes

Das neue Asylverfahrensgesetz läßt die erkenntungsdienstliche Behandlung aller Asylbewerber zu. Eine sachliche Notwendigkeit dafür ist nicht ersichtlich.

Alle Asylsuchenden machen falsche Angaben zur Person, vernichten ihre Legitimationspapiere und versuchen, durch mehrfache Asylanträge die Behörden zu täuschen; sie kommen in besonderem Maße als **Straftäter** in Betracht. Diesen Eindruck könnte man gewinnen, wenn man § 16 des Asylverfahrensgesetzes liest. Danach ist, von wenigen speziellen Ausnahmen abgesehen, in jedem Fall „die Identität eines Ausländers, der um Asyl nachsucht, durch erkenntungsdienstliche Maßnahmen zu sichern“.

Bereits im 14. Tätigkeitsbericht (S. 29) hatten wir darauf hingewiesen, daß die Praxis in der zentralen schleswig-holsteinischen Aufnahmestelle im Widerspruch zur früheren Gesetzeslage in nahezu jedem Fall zu einer erkenntungsdienstlichen Behandlung führte, obwohl dies nach damaliger Rechtslage nur bei Zweifeln im Einzelfall zulässig war. Darüber hinaus erschien die Aufnahme von Abdrucken **aller zehn Finger** nicht erforderlich, da eine eindeutige Identifizierung auch mit Hilfe eines einzigen Fingerabdrucks möglich ist.

Die Konferenz der Datenschutzbeauftragten hat sich mit großer Mehrheit gegen die Neuregelung gewandt. In einer EntschlieÙung wird auf die praktischen Erfahrungen hingewiesen und gefordert, entsprechend dem Gebot der Verhältnismäßigkeit staatlicher Eingriffe

- die erkenntungsdienstliche Behandlung auf konkrete Zweifelsfälle zu beschränken,
- den Umfang erkenntungsdienstlicher Unterlagen auf das Erforderliche zu beschränken und auf den Zehnfingerabdruck zugunsten des Einfingerabdrucks zu verzichten und schließlich
- die Nutzung des erkenntungsdienstlichen Materials für Zwecke der Strafverfolgung nicht voraussetzungslos zu gestatten, sondern von weiteren Bedingungen abhängig zu machen, etwa von dem Verdacht besonders schwerer und

enumerativ aufzuzählender Delikte. Bei polizeilicher Gefahrenabwehr wären ähnliche Regelungen zu treffen.

Diese Bedenken hat der Gesetzgeber nicht berücksichtigt.

4.1.4.2 Müssen sich Asylbewerber selbst strafbarer Handlungen bezichtigen?

Asylbewerber bezichtigen sich gelegentlich im Rahmen ihrer Anträge strafbarer Handlungen in ihrem Herkunftsland. Ausländer- oder Asylbehörden sollen nach bestehenden Verwaltungsvorschriften die Strafverfolgungsbehörden davon unterrichten. Eine ausreichende Rechtsgrundlage ist dafür jedoch nicht vorhanden.

In Arbeitskreisen der Polizei auf Bundesebene wurde gegenüber der allgemeinen Verwaltung darauf gedrängt, die Ausländer- bzw. Asylbehörden speziell auch im Hinblick auf Asylbewerber anzuhalten, ihrer Mitteilungspflicht gemäß den „Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten“ (RiVAST) nachzukommen. Diese sehen vor, daß eine Behörde von dem Verdacht, daß ein Ausländer im Ausland eine Straftat begangen habe, die Staatsanwaltschaft bei dem Oberlandesgericht benachrichtigt. Daß auch in diesem Fall die **Mitteilungsvorschriften** im Justizbereich als bloße **Verwaltungsvorschriften** keine ausreichende Rechtsgrundlage für Datenübermittlungen bieten, ist klar. Sogar einige Polizeibehörden der Länder teilen diese Meinung.

Ausländerbehörden unterliegen keinem allgemeinen Strafverfolgungszwang und sind so zur generellen Anzeige strafbarer Handlungen nicht verpflichtet. Die Verfolgung von **Auslandsstraftaten** nach dem StGB erfolgt ebenfalls **nicht** nach dem Legalitätsprinzip. Das Gesetz über die **internationale Rechtshilfe** in Strafsachen schließlich, das eine vorläufige Auslieferungshaft bei strafbaren Handlungen ermöglicht, geht von der Erwartung eines Auslieferungsersuchens aus und deckt gerade den Fall fehlender ausländischer Strafverfolgung nicht ab.

Folgerichtig wurde gefordert, in einer eindeutigen, normenklaren Rechtsvorschrift eine Grundlage für entsprechende routinemäßige Übermittlungen von Informationen über Auslandsstraftaten in einem Gesetz (z.B. im Ausländergesetz) zu schaffen.

Hier mußten wir gegenüber dem Justizminister und dem Innenminister allerdings **grundsätzliche Bedenken** deutlich machen. Ein Asylbewerber befindet sich häufig in einer schwierigen Lage. Er muß die Tatsachen darstellen, die seine Furcht vor politischer Verfolgung begründen und trägt das Risiko, daß ihm Asyl nicht gewährt wird, wenn seine Ausführungen für unzulänglich angesehen werden. Um Zweifel an der Glaubhaftigkeit seiner Darstellungen zu vermeiden, kann er sich genötigt sehen, auf eigene, politisch motivierte strafbare Handlungen im Herkunftsland hinzuweisen. Führen diese

Hinweise automatisch zu einer Information der Staatsanwaltschaft, so würde der Grundsatz in Frage gestellt, daß niemand gezwungen werden darf, **sich selbst** strafbarer Handlungen zu **bezichtigen**. In anderen Bereichen sind in vergleichbaren Konfliktfällen gesetzliche Lösungen gefunden worden. Sie bringen zum Ausdruck, daß das Interesse des Betroffenen daran, seine Angaben ausschließlich im zugrunde liegenden Verwaltungsverfahren verwertet zu sehen, gegen das Interesse der Allgemeinheit an der Verfolgung von Straftaten abzuwägen ist und daß für den Staat sogar eine Einschränkung des Strafverfolgungsanspruchs in Betracht kommt (z.B. im Sozialgesetzbuch).

Deshalb müßte eine zu schaffende gesetzliche Grundlage **Einschränkungen** zugunsten der Betroffenen vorsehen. So könnte die Zulässigkeit einer Übermittlung auf solche Strafverfahren beschränkt werden, die **erhebliche Rechtsgutverletzungen** (z.B. Verbrechen oder Straftaten der in § 138 StGB aufgezählten Art) oder strafbare Handlungen im Zusammenhang mit dem zugrunde liegenden Verwaltungsverfahren selbst zum Gegenstand haben. Darüber hinaus müssen **Aufklärungspflichten** festgelegt werden, die es dem Betroffenen ermöglichen, frei zu entscheiden, welche Angaben er machen will, und die ihm einen Überblick über die Rechtsfolgen geben, die mit seinen Angaben oder ihrer Verweigerung verbunden sind. Der Betroffene ist auch über Strafverfolgungsmöglichkeiten aufzuklären und darauf hinzuweisen, welche seiner Angaben in Strafverfahren gegen ihn verwendet werden können.

Die bundesweite Diskussion einer generellen Neufassung der RiVAST ist noch nicht abgeschlossen. Der Innenminister hält den gesamten Fragenkomplex ebenfalls für weiter erörterungsbedürftig und hat überdies Zweifel, ob die Forderung nach gesetzlicher Fixierung solcher Datenübermittlungen weiter verfolgt wird. Für diesen Fall hat er eine Berücksichtigung der Datenschutzargumente zugesichert.

4.1.5 Bau- und Wohnungswesen

Mietpreisspiegel: Datenschutz beinahe übersehen

Für die Aufstellung eines Mietspiegels ließ sich eine Stadt Kundendaten der Stadtwerke übermitteln. Die Verwendung der Daten für diesen Zweck ist nur mit Einwilligung der Kunden zulässig.

Um Fehlentwicklungen bei der Mietpreisgestaltung auf dem Wohnungsmarkt entgegenzuwirken, sollte für eine kreisfreie Stadt ein **Mietpreisspiegel** aufgestellt werden. Als Grundlage zur Durchführung der notwendigen Befragung der Mieter bzw. Vermieter griff man auf die Kundendatei der Stadtwerke zurück, da die Einwohnermeldedatei für diesen Zweck nicht hinreichend strukturiert war. Datenschutzrechtliche Bedenken

hinsichtlich dieser Datenübermittlung kamen jedoch erst nach Abschluß aller Vorarbeiten auf.

Da die Stadtwerke in privatrechtlicher Form organisiert waren, mußten natürlich auch die Vorschriften des **Bundesdatenschutzgesetzes** beachtet werden. Danach ist unter anderem eine Weitergabe personenbezogener Daten, die nicht im Rahmen des Vertragszweckes stattfindet, nur zulässig, soweit sie zur Wahrnehmung öffentlicher Interessen erforderlich ist und kein Grund zu der Annahme besteht, daß Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung haben. Problematisch war hier vor allem, ob die Kunden der Stadtwerke ein solches **schutzwürdiges Interesse** geltend machen können. Dies war anzunehmen, da sich der Mietpreisspiegel im Einzelfall für Betroffene mit einer sehr günstigen Miete auch negativ auswirken kann, erleichtert er doch in diesen Fällen das Verfahren für eine Mieterhöhung erheblich.

Eine ausreichende Wahrung der Rechte der Betroffenen konnte schließlich nur dadurch gewährleistet werden, daß die übermittelten Daten zunächst nur dazu genutzt wurden, vor einer weiteren Verarbeitung die Einwilligung der Betroffenen zu der beabsichtigten Datenverarbeitung einzuholen. Wurde sie verweigert, erfolgte die sofortige Löschung der Daten. Die **Einholung der Einwilligung** konnte auf Anraten des Landesbeauftragten gerade noch rechtzeitig vor der Weiterverarbeitung der Daten zwischengeschaltet werden. Wären die Kundenadressen ohne entsprechende Einwilligung genutzt worden, hätte dies eine Rechtspflicht zur Löschung der bereits verarbeiteten Daten zur Folge gehabt. Die bis dahin angefallenen Kosten für den Mietpreisspiegel wären verloren gewesen.

4.2 Kommunalrecht

4.2.1 Erste Erfahrungen bei der Anwendung des neuen Datenschutzrechts

Kommunalverwaltungen haben noch Probleme mit den neuen Bestimmungen des LDSG. Insbesondere bei der Information der Bürger bei freiwilligen Umfragen, bei der Beachtung der Zweckbindung und bei der Transparenz der Datenverarbeitung für die Betroffenen bestehen Defizite.

Auch das neue Landesdatenschutzgesetz geht von dem Grundsatz aus, daß die Verarbeitung personenbezogener Daten generell unter Erlaubnisvorbehalt steht und entweder der Einwilligung des Betroffenen oder einer normenklaren Rechtsvorschrift als Ermächtigungsgrundlage bedarf. Im Selbstverwaltungsbereich der Kommunen haben sich in diesem Punkt Schwierigkeiten ergeben.

Daß der Verwaltung nicht nur die zu erfüllenden Aufgaben zu übertragen sind, sondern gleichzeitig auch zu regeln ist, in welchem Umfang in diesem Zusammenhang personenbezogene Daten verarbeitet werden dürfen, ist im **kommunalen Sat-**

zungsrecht bisher nur spärlich berücksichtigt. Auch eine Verwendung von Daten, die die Kommune in anderem Sachzusammenhang erhoben hat, ist nach dem Zweckbindungsgrundsatz des LDSG nur noch möglich, wenn dafür eine ausdrückliche Befugnis z. B. im Satzungsrecht vorhanden ist. Die nachfolgenden Beispiele aus der Praxis verdeutlichen die aufgetretenen Schwierigkeiten.

4.2.1.1 Einführung einer Sozialstaffel für Elternbeiträge im Kindergarten

Ohne ausreichende Erläuterung der Freiwilligkeit, des Zwecks und des Verfahrens der Umfrage ist eine Erhebung von Daten über Einkommensverhältnisse unzulässig.

In einer Stadt war beabsichtigt, im Rahmen der Förderung von Kindergartenplätzen eine **Sozialstaffel** für die zu erhebenden Elternbeiträge einzuführen. Die Höhe der Förderung an den privaten Kindergartenträger sollte künftig von den wirtschaftlichen Verhältnissen der Eltern abhängig gemacht werden. Da man über keinerlei Berechnungsgrundlagen für die Ausgestaltung der Sozialstaffel verfügte, startete man noch vor der Beschlußfassung über die Satzung eine **Umfrageaktion** bei den Eltern. Bei dieser Datenerhebung wurde offengelassen, ob die Preisgabe der Daten auf freiwilliger Grundlage erfolgen sollte. Viele Betroffene haben in Anbetracht des bestehenden Abhängigkeitsverhältnisses die geforderten Daten geliefert, wollten sie doch bei der Verteilung der knappen Kindergartenplätze kein Risiko eingehen.

Die datenschutzrechtliche Prüfung auf Wunsch einiger Eltern ergab, daß keine ausreichende Ermächtigungsgrundlage zur Datenverarbeitung vorhanden war, da weder eine rechtswirksame **Einwilligung** der Betroffenen noch eine **rechtskräftige** Satzung vorlag. Die von der Stadt in unzulässiger Weise verarbeiteten Daten mußten gelöscht werden.

4.2.1.2 Führung eines kommunalen Grundstückseigentümerverzeichnisses und Zweckbindung der Daten

Immer mehr Gemeinden gehen dazu über, Verzeichnisse über Grundstückseigentümer anzulegen. Hierfür bedarf es ausreichender Rechtsgrundlagen, die sich auch aus kommunalen Satzungen ergeben können.

Ob es um die Festsetzung von Erschließungsbeiträgen, Kanalbenutzungsgebühren, die Umsetzung einer Baumschutzsatzung oder ähnliches geht, die Kommunen benötigen häufig zur Erfüllung ihrer Aufgaben Angaben über die Eigentumsverhältnisse an Grundstücken. Um sich eine Vielzahl von zeitaufwendigen Anfragen beim Grundbuchamt zu ersparen, werden in vielen Verwaltungen sogenannte **Grundstückseigentümerverzeichnisse** geführt. Grundsätzlich bestehen aus datenschutzrechtlicher Sicht keine Bedenken hiergegen, wenn dafür

eine Rechtsgrundlage besteht. Diese kann sich auch aus kommunalem Satzungsrecht ergeben. Aus der Regelung muß hervorgehen, daß die Gemeinde ein Grundstückseigentümerverzeichnis führen darf, aufgrund welcher Datenquellen dieses Verzeichnis aufgestellt und aktualisiert wird, sofern sich dies nicht bereits aus anderen Vorschriften ergibt, und zu welchen Zwecken es genutzt werden soll.

Zur Aktualisierung dieser Verzeichnisse greifen viele Gemeinden z.B. auf die **Grundstückskaufverträge** zu, die ihnen zur Ausübung des Vorkaufsrechts nach dem Baugesetzbuch zur Verfügung gestellt werden. Dabei ist aber zu bedenken, daß sich aus diesen Verträgen die Eigentumsverhältnisse nicht zuverlässig ergeben. Werden sie gleichwohl in der beschriebenen Weise genutzt, so liegt darin eine Zweckänderung, die in der Satzung geregelt sein muß.

Ähnliche Fragestellungen ergeben sich, wenn in dieser Weise auf bereits vorhandene **Bauakten** zugegriffen werden soll sowie wenn Daten über den Frischwasserbezug, die zunächst nur für die Berechnung der Wassergebühren erhoben werden, gleichzeitig für die Berechnung der Abwassergebühren zugrunde gelegt werden sollen.

4.2.1.3 **Transparenz der Datenverarbeitung für den Bürger**

Der Bürger muß bei der Datenerhebung über deren Zweck und weitere Einzelheiten aufgeklärt werden. Verletzungen des Transparenzgebotes können empfindliche Auswirkungen haben.

Um den Bürger über die Verwendung seiner Daten bei der datenverarbeitenden Stelle zu unterrichten, wurde in das Datenschutzrecht die Verpflichtung für die Behörden aufgenommen. Betroffene bereits bei der Datenerhebung über die Ermächtigungsgrundlage sowie über Zweck und Umfang der Datenverarbeitung im Einzelfall **aufzuklären**. Daraus folgt, daß er zum frühestmöglichen Zeitpunkt informiert werden muß, wenn die Daten bei anderen Stellen und ohne seine Kenntnis erhoben werden. Versäumnisse in dieser Hinsicht können unter Umständen spürbare Auswirkungen für die Behörde mit sich bringen, wie das nachfolgende Beispiel zeigt.

In manchen Gemeinden müssen Vermieter die **Kurverwaltung** unterrichten, wenn ihnen der Gast keine Kurkarte vorlegt. Die Gemeinde darf diese Daten nur verwenden, wenn sie den Kurgast umgehend über die Datenerhebung unterrichtet. Anderenfalls sind die Daten zu löschen und die Kurabgabe geht verloren.

Um eine umfassende Überwachung der Kurabgabenerhebung zu gewährleisten, wurden in einer Kommune die Kurgäste durch die Kurabgabesatzung verpflichtet, ihre Kurkarte innerhalb von 24 Stunden nach Ankunft dem örtlichen Vermieter vorzulegen. Wurde dies versäumt, war der Vermieter ver-

pflichtet, eine **Kontrollmitteilung** an die Kurverwaltung zu fertigen.

Ein Kurgast bezweifelte, daß für ihn überhaupt eine Verpflichtung zur Zahlung der Kurabgabe bestand. Da er weder zur Zahlung aufgefordert oder gar gemahnt wurde, sah er auch keine Veranlassung, sich deshalb mit der Kurverwaltung auseinanderzusetzen. Was er jedoch nicht wußte, war, daß sein Vermieter nach Ablauf der 24-Stundenfrist eine Kontrollmitteilung schrieb. Um so mehr mußte es ihn überraschen, als er zwei Monate nach seinem Aufenthalt in Schleswig-Holstein plötzlich einen Nachveranlagungsbescheid zur Kurabgabe in den Händen hielt.

Nach dem **Transparenzgebot** des LDSG war die Kurverwaltung verpflichtet, den Betroffenen über die Datenerhebung beim Vermieter, die ja ohne seine Kenntnis erfolgt ist, aufzuklären. Da dies nicht geschehen ist, sind die Daten in unzulässiger Weise erhoben worden und durften deshalb nicht gespeichert bzw. mußten gelöscht werden. Die Kenntnis über Name und Anschrift des Betroffenen war damit für die Behörde unwiederbringlich verloren. Dem Kurabgabebescheid war mit der Löschung der Daten des Adressaten die entscheidende Grundlage entzogen.

Gerade dieser Fall zeigt, daß es sich bei dem Transparenzgebot des LDSG um mehr als nur um einen rein formalen Akt handelt. Wäre der Betroffene frühzeitig über das auf der Grundlage der Kurabgabebesatzung durchgeführte Kontrollverfahren unterrichtet worden, hätte er rechtzeitig noch während seines Ferienaufenthaltes klären können, ob und gegebenenfalls in welchem Umfang tatsächlich eine Kurabgabepflicht bestand. So aber ist er davon ausgegangen, daß er sich diesem Problem gar nicht zu stellen brauchte. Bei einer ordnungsgemäßen Beachtung des Transparenzgebotes dürfte sich ohnehin der Anteil der Kurgäste, die ihre Kurabgabe nicht rechtzeitig bezahlen, erheblich verringern lassen. Für die Kurverwaltung dürfte dadurch im Ergebnis sogar ein wirtschaftlicher Vorteil erreicht werden können.

4.2.2 Datenschutz bei Beratungen der Gemeindevertretung: nicht ausgerechnet gegen den Betroffenen

Betroffene können nicht mit der Begründung von der Teilnahme an nichtöffentlichen Beratungen kommunaler Entscheidungsgremien ausgeschlossen werden, der Schutz ihrer eigenen berechtigten Interessen gebiete eine vertrauliche Beratung.

Nach der Gemeindeordnung ist die **Öffentlichkeit** von **Sitzungen** der Gemeindevertretung und von Ausschüssen dann auszuschließen, wenn „... berechnete Interessen einzelner es erfordern“. Ob das der Fall ist, muß anhand des Beratungsgegenstandes und des anzuwendenden Verfahrensrechts entschieden werden. Beispielsweise gelten für Bauanträge neben

baurechtlichen Spezialvorschriften, die das baurechtliche Einvernehmen der Gemeinde fordern, und dem kommunalen Verfahrensrecht, das eine Beratung in der Gemeindevertretung bzw. in Ausschüssen vorsehen mag, auch die Vorschriften des Landesverwaltungsgesetzes. Danach haben die Verfahrensbeteiligten einen Anspruch darauf, daß ihre zum persönlichen Lebensbereich gehörenden Geheimnisse von der Behörde nicht unbefugt offenbart werden. Bei der Behandlung von **Bauanträgen** geht es in den meisten Fällen um den persönlichen Lebensbereich des Antragstellers und um Sachverhalte, die nicht jedermann zur Kenntnis kommen sollen. Der Vertraulichkeitsschutz nach dem Landesverwaltungsgesetz überwiegt daher. Bauanträge sind deshalb nicht öffentlich zu behandeln. Dies darf sich aber nicht gegen den Betroffenen selbst richten.

Trotz Ausschlusses der Öffentlichkeit zum Schutz ihrer Interessen dürfen daher **Betroffene** an der nichtöffentlichen Sitzung **teilnehmen**. Der Hinweis mancher Gemeinde auf den Datenschutz oder auf die Sicherung der schutzwürdigen Interessen der Betroffenen geht in diesen Fällen fehl; denn es erscheint widersinnig, sie vor sich selbst schützen zu wollen. Ihrer Anwesenheit bei der Beratung ihrer Angelegenheit in nichtöffentlichen Sitzungen stehen daher datenschutzrechtliche Bedenken nicht entgegen, wenn folgende Grenzen eingehalten werden:

- Die Anwesenheit des Betroffenen ist nicht zugelassen, wenn die Gemeindevertretung, was nach der Gemeindeordnung möglich ist, generell die Öffentlichkeit von Ausschusssitzungen ausgeschlossen hat.
- Die Anwesenheit des Betroffenen kommt auch nicht in Betracht, wenn zusätzlich die berechtigten Interessen weiterer Personen oder überwiegende Belange des öffentlichen Wohls berührt sein können. Zumindest muß der Betroffene vor dem Beratungsstadium, in dem die weiteren Privatinteressen oder die Belange des öffentlichen Wohls zur Sprache kommen, ausgeschlossen werden.
- Schließlich darf das Anwesenheitsrecht des Betroffenen nicht zur einer Teilöffentlichkeit der Sitzung für weitere ihm genehme Personen führen. Das könnte den unbeeinflussten, neutralen Ablauf der Sitzung und die Objektivität der Beschlußfassung beeinträchtigen.

Unseren Überlegungen hat sich inzwischen auch der Innenminister angeschlossen. Er hat die kommunalen Aufsichtsbehörden entsprechend unterrichtet. Offen geblieben sind noch Detailfragen über die Vertretung Betroffener bei Abwesenheit bzw. über ihre rechtliche Beratung. Hierzu werden weitere Abstimmungsgespräche geführt.

4.3 Justizverwaltung

4.3.1 Geltung des Landesdatenschutzgesetzes im Justizbereich

Das Landesdatenschutzgesetz gilt grundsätzlich in vollem Umfang für Staatsanwaltschaften und Gerichte. Nur bereichsspezifische Vorschriften über die Datenverarbeitung gehen vor. Von der Kontrolle durch den Landesbeauftragten sind nur Gerichte ausgenommen, soweit sie Rechtsprechung ausüben.

Die Geltung des Landesdatenschutzgesetzes auch für den Bereich der Justiz war im Gesetzgebungsverfahren umstritten. Der Regierungsentwurf hatte noch weitgehende Ausnahmen vorgesehen, die dann vom Landtag gestrichen wurden. Nach dem vom Parlament verabschiedeten Text kann es nicht zweifelhaft sein, daß das **Landesdatenschutzgesetz** grundsätzlich in vollem Umfang von **Gerichten** und **Staatsanwaltschaften anzuwenden** ist. Ausnahmen gelten nur, „soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln“. Außerdem unterliegen die Gerichte unserer Kontrolle nicht, soweit sie „in richterlicher Unabhängigkeit tätig werden“. Von diesen beiden Ausnahmen abgesehen, ist das LDSG sowohl von der Staatsanwaltschaft als auch von den Gerichten anzuwenden wie von den anderen Behörden des Landes auch.

In der Praxis ergeben sich aber offenbar immer wieder **Auslegungsschwierigkeiten**. Auch im Berichtszeitraum wurden wir mehrfach mit Anfragen und Sachverhalten befaßt, die letztlich auf die Frage hinausliefen, ob nicht in diesem oder jenem Fall Staatsanwaltschaft und Justiz von der Geltung des Landesdatenschutzgesetzes ausgenommen seien.

So stellte der Generalstaatsanwalt in einem Schreiben an den Justizminister die Frage, inwieweit das **Auskunfts- und Akteneinsichtsrecht** nach dem LDSG auch von den **Staatsanwaltschaften** zu respektieren sei. Zunächst einmal ergebe sich nämlich ohne Berücksichtigung der bereits bestehenden oder künftigen Regelungen der Strafprozeßordnung und ohne Berücksichtigung der Rechtslage hinsichtlich der Regelungszuständigkeit das „zumindest verwirrende Bild“, daß jeder, dessen personenbezogene Daten in staatsanwaltschaftlichen Akten oder Dateien gespeichert sind, grundsätzlich einen Anspruch auf Akteneinsicht oder zumindest auf Auskunftserteilung habe. Dies könne in dieser Reichweite nicht richtig sein. Im weiteren führt der Generalstaatsanwalt dann aus, daß im Rahmen der Strafprozeßordnung der Beschuldigte nur über seinen Verteidiger Akteneinsicht nehmen könne. Zumindest bei laufenden Ermittlungsverfahren müsse diese Regelung Vorrang vor den Auskunfts- und Akteneinsichtsrechten des LDSG haben. Soweit die Strafprozeßordnung keine Regelung über Akteneinsichtsrechte enthalte, etwa wenn es sich um Dritte, Zeugen etc. handle, müßten die untergesetzlichen Vorschriften, z.B. der Richtlinien für das Strafverfahren und das

Bußgeldverfahren (RiStBV) übergangsweise Vorrang vor den landesgesetzlichen Regelungen haben.

Dem haben wir widersprochen. Der **Übergangsbonus** ist eine nirgendwo exakt geregelte, lediglich aus einigen Urteilen des Bundesverfassungsgerichts abgeleitete Rechtsfigur. Sie hat nur dort ihre Bedeutung, wo sich aus Urteilen des Bundesverfassungsgerichts die Rechtswidrigkeit einer bestehenden Regelung oder die Notwendigkeit zur Schaffung einer Neuregelung ergibt und gleichwohl die Verwaltung im unbedingt notwendigen Rahmen weiterarbeiten muß. Bestehen aber verfassungsgemäße landesgesetzliche Regelungen, so ist für die Anwendung des Übergangsbonus kein Platz. Dies gilt auch dann, wenn vermutet wird, daß der Bundesgesetzgeber eine vom Landesgesetzgeber in Details abweichende Regelungen treffen könnte. Deshalb besteht für eine Berufung auf den Übergangsbonus in Verbindung mit den RiStBV kein Raum, da Auskunfts- und Akteneinsichtsrechte der Betroffenen im LDSG klar und präzise geregelt sind.

Weiter haben wir dargelegt, daß der Anspruch auf **Auskunft** und **Akteneinsicht** nach dem LDSG eine **andere Zielrichtung** verfolgt als die strafprozessualen Akteneinsichtsrechte. Letztere bestehen zu dem Zweck, dem Beschuldigten eine angemessene Vorbereitung auf die Verteidigung zu ermöglichen. Der datenschutzrechtliche Auskunfts- und Akteneinsichtsanspruch erwächst allein aus der Tatsache, daß Daten über die betreffende Person gespeichert sind.

Auch vom datenschutzrechtlichen Auskunfts- und Akteneinsichtsanspruch gibt es **Ausnahmen**. So ist es beispielsweise möglich, die Akteneinsicht dann zu verweigern, wenn dadurch **laufende Ermittlungen** gefährdet würden. Letztlich kann der Beschuldigte insoweit auf dem Umweg über das datenschutzrechtliche Auskunftsrecht nicht mehr erfahren, als ihm nach dem strafprozessualen Akteneinsichtsrecht zusteht.

Allerdings kann er sein datenschutzrechtliches Auskunfts- und Akteneinsichtsrecht selbst und ohne **anwaltliche Vertretung** in Anspruch nehmen. Für den strafprozessualen Akteneinsichtsanspruch ist es hingegen herrschende Auffassung, daß er nur über den Anwalt geltend gemacht werden kann. Da es aber ebenso unbestritten ist, daß der Anwalt befugt ist, aus den Akten Kopien zu fertigen und an den Beschuldigten weiterzugeben, kann dieser im Rahmen der strafprozessualen Akteneinsicht ebenfalls Kenntnis vom Inhalt der ihn betreffenden Datenspeicherung erhalten. Allerdings entstehen dabei Anwaltsgebühren.

Der datenschutzrechtliche Auskunfts- und Akteneinsichtsanspruch nach dem LDSG ist hingegen **gebührenfrei**. Es würde deshalb eine Umgehung des Anspruchs auf gebührenfreie Auskunft bedeuten, würde man den Betroffenen stets auf den Umweg über die anwaltlich vermittelte Akteneinsicht nach der Strafprozeßordnung verweisen. Wir haben deshalb im Ergebnis keinen Zweifel, daß der datenschutzrechtliche Auskunfts- und Akteneinsichtsanspruch grundsätzlich auch gegenüber der

Staatsanwaltschaft gilt. Er findet seine Begrenzung lediglich in den im LDSG enthaltenen allgemeinen Gründen der Auskunftsverweigerung, etwa wenn dadurch laufende Ermittlungen gefährdet würden.

Der Justizminister hat sich zu der Angelegenheit noch nicht abschließend geäußert. Er will erst das Ergebnis einer **Umfrage des Generalstaatsanwalts** bei den Behörden seines Geschäftsbereiches abwarten, bei der Art und Zahl der im vergangenen Jahr gestellten Auskunftersuchen ermittelt werden sollen.

Ein anderer Schriftwechsel mit dem Justizminister mußte zur Frage der **Kontrollkompetenz** des Datenschutzbeauftragten gegenüber den **Gerichtsvollziehern** geführt werden. Der Justizminister hatte sich auf den Standpunkt gestellt, daß die Gerichtsvollzieher, soweit sie als selbständiges Organ der Rechtspflege tätig werden, nicht der Kontrolle des Datenschutzbeauftragten unterliegen. Er hatte sich für diese Rechtsauffassung auf die Entstehungsgeschichte der Kontrollvorschriften des neuen LDSG berufen, aus denen sich ergebe, daß eine Erweiterung der Kontrollkompetenz des Datenschutzbeauftragten gegenüber der früheren Rechtslage nicht beabsichtigt gewesen sei. Zum früher hierfür einschlägigen Paragraphen des LDSG habe er aber immer die Auffassung vertreten, daß er eine datenschutzrechtliche Kontrolle bei den Gerichtsvollziehern nicht zulasse.

Demgegenüber haben wir auf den **klaren Wortlaut** des neuen LDSG verwiesen. Danach sind nur die Gerichte und nur, soweit sie in richterlicher Unabhängigkeit tätig werden, von der Kontrolle ausgenommen. Gerichtsvollzieher sind weder „Gerichte“, noch werden sie in „richterlicher Unabhängigkeit“ tätig. Im übrigen gibt es auch kein nachvollziehbares sachliches Bedürfnis, die bei Gerichtsvollziehern betriebenen **sensiblen Datensammlungen** der Kontrolle zu entziehen. Inzwischen konnte mit dem Justizminister Einigung erzielt werden, daß auch die Gerichtsvollzieher der datenschutzrechtlichen Kontrolle unterliegen. Bei der praktischen Durchführung von Kontrollen soll der **Weisungsunabhängigkeit** der Gerichtsvollzieher soweit möglich Rechnung getragen werden. Dies soll in der Form geschehen, daß in Querschnittskontrollen möglichst nicht laufende Vollstreckungsverfahren einbezogen werden und daß bei der Abfassung des Prüfberichts mehr auf die Darstellung der generellen Verfahrensweise als einzelner Fälle Wert gelegt wird.

Im Zusammenhang mit Plänen zur Schaffung **privater Bundesschuldnerverzeichnisse** stellte sich die Frage, inwiefern die Vorschriften des Landesdatenschutzgesetzes einer Übermittlung von Daten aus den Schuldnerverzeichnissen der Amtsgerichte an derartige Stellen entgegenstehen. Der Grundsatz der Zweckbindung sowie die Regelungen über die Übermittlung von personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereichs könnten im Ergebnis dazu führen, daß eine Datenübermittlung zu diesem Zweck nicht zulässig ist.

Der Justizminister stellte sich jedoch auf den Standpunkt, daß das LDSG neben den Vorschriften der Zivilprozeßordnung nicht anwendbar sei. Zwar habe das Gesetz Vorrang, soweit nicht besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln. Es sei auch einzuräumen, daß die Zivilprozeßordnung keine abschließende Regelung enthält. Die hierzu ergangene zusätzliche allgemeine Vorschrift des Bundesministers der Justiz über die Erteilung und die Verbreitung von Abschriften oder Auszügen aus den Schuldnerverzeichnissen vom 1. August 1955 könne aber übergangsweise als „gesetzliche Grundlage“ im Sinne des LDSG angesehen werden.

Dem ist aus unserer Sicht zu widersprechen. Eine Verwaltungsvorschrift aus den 50er Jahren kann nicht gegenüber dem LDSG als vorrangige Rechtsgrundlage akzeptiert werden.

4.3.2 **Geschäftsstellenautomation der Staatsanwaltschaft (GAST): Verbesserungen werden wirksam**

Der Generalstaatsanwalt zieht Konsequenzen aus der datenschutzrechtlichen Kritik an GAST. Ein Teil der Verbesserungen ist bereits umgesetzt. Es bleiben die Defizite hinsichtlich der Rechtsgrundlage für GAST.

In den letzten beiden Tätigkeitsberichten (13. TB, S. 42, 14. TB, S. 38) haben wir über unsere **Querschnittskontrolle** der Geschäftsstellenautomation der Staatsanwaltschaft (GAST-SH) berichtet. Dort ist im einzelnen dargelegt worden, welche Mängel wir bei unserer Kontrolle festgestellt haben, in welchen Fällen der Generalstaatsanwalt Abhilfe zugesagt hat und in welchen Punkten ein Dissens geblieben ist.

Inzwischen hat der Generalstaatsanwalt mitgeteilt, welche **Maßnahmen** im vergangenen Jahr **ergriffen** worden sind. Eine Reihe von Verbesserungen sind bereits wirksam geworden bzw. stehen kurz vor der Realisierung. Von zentraler Bedeutung ist dabei die **Begrenzung des Zugriffs** zu den in GAST gespeicherten Daten auf die Staatsanwaltschaft, bei der das Ermittlungsverfahren anhängig ist oder gewesen ist, in folgenden Fallgruppen:

- Verfahren, in denen von der Einleitung eines Ermittlungsverfahrens mangels jeglichen Anfangsverdachts abgesehen worden ist,
- Verfahren, denen eine böswillige bzw. querulatorische Anzeige zugrunde lag,
- Verfahren, in denen mangels Ermittlung eines Täters die Personendaten des Geschädigten/Anzeigenden in GAST gespeichert worden sind,
- Verfahren, die eine Sexualstraftat zum Gegenstand haben und bei denen mangels Ermittlung des Täters die Personalien des Opfers in abgekürzter Form in GAST eingestellt worden sind,

- Verfahren, die einen unnatürlichen Tod ohne Fremdeinwirkung (z.B. vollendete Selbsttötung) betreffen,
- Verfahren, in denen Strafunmündige als Beschuldigte gespeichert sind,
- in der Regel Verfahren, in denen rechtskräftig ein Freispruch ergangen ist.

Die Beendigung des landesweiten Zugriffs auf derartige Datensätze ist im Januar dieses Jahres erfolgt. Damit ist in diesen Fällen eine wichtige Forderung aus den Prüfungen erfüllt und das Prinzip des landesweiten Zugriffs auf die in GAST gespeicherten Daten insoweit durchbrochen. Die noch weitergehende Zugriffsbeschränkung auf das die Ermittlungen führende Dezernat, sofern im Datensatz die Daten von **Opfern von Sexualstraftaten** gespeichert sind, soll ebenfalls Anfang 1993 wirksam werden.

Den **Dezernenten** wurde Ende 1992 ein „datenschutzrechtliches Kontrollblatt“ an die Hand gegeben, mit dem in jeder Handakte zu dokumentieren ist, daß der Dezernent sich nach Abschluß der Ermittlungen sowie des gerichtlichen Verfahrens vergewissert hat, ob die in GAST gespeicherten Daten tatsächlich noch zutreffend sind.

Der **Katalog der Erledigungs- und Entscheidungsarten** wurde überarbeitet und verfeinert. Nunmehr ist es leichter möglich, den Abschluß eines Ermittlungsverfahrens korrekt in GAST darzustellen. Dadurch können unnötige Belastungen der Betroffenen vermieden werden.

In der Vergangenheit wurden die Daten der **Opfer von Verkehrsunfällen** häufig wie die eines Täters gespeichert. Dies wird künftig unterbleiben. Derzeit werden die Daten der bislang in dieser Form erfaßten Personen gelöscht.

Die notwendigen Änderungen sind auch bezüglich der Speicherung von Daten im Zusammenhang mit versuchter oder vollendeter **Selbsttötung** realisiert. Versuchte Selbsttötung wird von der Polizei nur noch dann an die Staatsanwaltschaft gemeldet und dementsprechend in GAST erfaßt, wenn konkrete Anhaltspunkte einer Fremdeinwirkung vorliegen. Statt als „versuchte Selbsttötung“ werden die Verfahren in diesen Fällen nur noch als „sonstige Verfahren“ gespeichert. Vollendete Selbsttötungen werden künftig nur noch unter der Kennzeichnung „unnatürlicher Tod“ erfaßt.

Das Datenfeld „**besondere Hinweise**“, in dem in der Vergangenheit gelegentlich belastende Bewertungen bezüglich des Tatverdächtigen sowie alte Aktenzeichen über bereits gelöschte Akten erfaßt wurden, ist abgeschafft.

In den noch verbliebenen offenen Punkten ist es zu keiner weiteren Annäherung der Standpunkte gekommen. Dies betrifft insbesondere den **generellen landesweiten Zugriff** auf die in GAST gespeicherten Daten als Regelfall. Nach unserer Auffassung besteht für das GAST-Verfahren derzeit keine den Anforderungen des Bundesverfassungsgerichts entsprechende

bereichsspezifische, präzise **Rechtsgrundlage**. Demgemäß darf das Verfahren nur noch zeitlich befristet und unter den engen Voraussetzungen, die nach der Rechtsprechung zum sogenannten „**Übergangsbonus**“ zu beachten sind, fortgeführt werden. Dies bedeutet insbesondere, daß das Verfahren sich auf das für die Strafrechtspflege unbedingt Erforderliche beschränken muß. Da Schleswig-Holstein das einzige Flächenland ist, das ein landesweites staatsanwaltschaftliches Dateiverfahren dieser Art betreibt, dürfte es nicht einfach sein, zu begründen, daß ohne ein Verfahren mit derartigem Zuschnitt eine geordnete Strafrechtspflege nicht möglich ist. In diesem Falle würde sich die Frage stellen, wie es den Staatsanwaltschaften in den anderen Flächenstaaten möglich ist, Strafverfolgung ohne ein Verfahren wie GAST zu betreiben.

Wir haben keine Möglichkeit, unseren Standpunkt in dieser Frage durchzusetzen. Es bleibt im Augenblick abzuwarten, wie die Gerichte, die derzeit mit einigen Klagen gegen GAST befaßt sind, entscheiden.

Auch in einem anderen wichtigen Punkt des Prüfberichts gibt es kaum Fortschritte. Die **Dauer der Speicherung** von Daten in GAST hängt unter anderem von den Fristen ab, die in den bundeseinheitlichen Aufbewahrungsbestimmungen für Unterlagen bei der Justiz vorgesehen sind. Der Generalstaatsanwalt sah in seiner ersten Stellungnahme zum Prüfbericht keine Möglichkeit, von diesen bundesweit geltenden Verwaltungsvorschriften abzuweichen. Er verwies aber darauf, daß der Justizminister Bestrebungen eingeleitet habe, die Aufbewahrungsbestimmungen bundeseinheitlich zu verkürzen. Wir haben daraufhin unsererseits unsere Kollegen in den anderen Bundesländern gebeten, unsere Position in Gesprächen mit den dortigen Justizministern zu unterstützen. Allerdings war in den übrigen Landesjustizministerien nirgendwo etwas von einer schleswig-holsteinischen Initiative zur datenschutzrechtlichen Verbesserung der Aufbewahrungsbestimmungen bekannt. Der Justizminister teilte nunmehr auf Anfrage mit, er habe sich noch nicht an die anderen Länder gewandt, weil er erst hausintern seine Position klären wolle.

4.3.3 Konsequenzen aus den Kontrollen in den Justizvollzugsanstalten kommen in Gang

Der Justizminister hat zum Prüfbericht über die Datenverarbeitung in den Justizvollzugsanstalten erste Stellungnahmen abgegeben. Darin werden überwiegend Verbesserungen zugesagt. Zu zentralen Kritikpunkten steht die Stellungnahme noch aus.

Im 14. Tätigkeitsbericht (S. 44) war von Querschnittskontrollen in den **Justizvollzugsanstalten** Kiel und Lübeck berichtet worden. Wir haben im Laufe des vergangenen Jahres mehrfach in Vortragsveranstaltungen vor Bediensteten der Justizvollzugsanstalten unsere Kritik näher begründet und mit den Praktikern die notwendigen Konsequenzen aus der Prüfung

erörtert. Zwischenzeitlich ist eine **erste Stellungnahme** des Justizministers eingegangen. Sie greift einige der Kritikpunkte auf, bezieht sich aber noch nicht auf die im Prüfbericht angesprochenen zentralen Fragen. Die Stellungnahme befaßt sich im wesentlichen mit der besseren Organisation einzelner Datenverarbeitungsverfahren. Es wurden eine Reihe von Maßnahmen angekündigt, bei deren Realisierung unbeabsichtigte und unnötige Datenoffenbarungen vermieden werden können.

So hat der Justizminister mitgeteilt, daß die auf den **Stationszimmern** vorhandenen **Hinweistafeln**, auf denen sämtliche in der jeweiligen Station einsitzenden Gefangenen mit einer Reihe von Daten verzeichnet sind, künftig durch eine geeignete Vorrichtung, wie etwa ein Rollo, abgedeckt werden. Darüber hinaus werde darauf geachtet, daß außer den Abteilungsbeamten nach Möglichkeit Unbefugte keinen Einblick nehmen könnten. Der Name des Gefangenen werde künftig auf der **Hafttraumbeschilderung** nicht mehr geführt, es sei denn, der Gefangene selbst bringe von sich aus ein Namensschild an. Dieses werde aber bei Anstaltsbesichtigungen umgedreht.

Das Verfahren der **erkennungsdienstlichen Behandlung** von Gefangenen wird in einigen Detailpunkten verbessert. Z. B. werden die Gefangenen bei Haftentlassung auf ihr gesetzliches Recht hingewiesen, die Vernichtung der ererkennungsdienstlichen Unterlagen zu verlangen. Die Weitergabe ererkennungsdienstlicher Unterlagen wird künftig dokumentiert, so daß einem begründeten Vernichtungsverlangen auch vollständig nachgekommen werden kann. Die Aufnahme von Fotos aus der ererkennungsdienstlichen Behandlung in Arztakten wird eingestellt.

Verbessert werden soll auch die Behandlung **sensibler Daten** über besondere Maßnahmen gegenüber Gefangenen. Solche Maßnahmen können zum Beispiel bei **Gefahr der Selbsttötung** oder der Gefährdung Dritter notwendig sein. Derartige Behandlungshinweise sollen künftig in Karteiform notiert und bei Erledigung der Maßnahme vernichtet werden.

Die **Gefangenenpersonalkartei** in der Zentrale der JVA Kiel soll um die Fälle bereits entlassener Gefangener bereinigt werden. Darüber hinaus soll sichergestellt werden, daß **Gefangenenpersonalakten**, die älter als 30 Jahre sind, entweder vernichtet oder dem Archiv angeboten werden. Außerdem sollen die Justizvollzugsanstalten generell dafür sorgen, daß Karteikarten, soweit sie nicht bei Haftentlassung ohnehin zu vernichten sind, zur Gefangenenpersonalakte des Betroffenen genommen werden.

Eine Reihe von bislang in **Buchform** geführten Verzeichnissen soll künftig so organisiert werden, daß eine Bereinigung nach Jahrgängen möglich ist. Bislang begann die Frist für die Bereinigung erst zu laufen, wenn ein Buch vollgeschrieben war, was unter Umständen erst nach Jahrzehnten der Fall war.

Die Verteilung von Informationen innerhalb der Anstalten soll restriktiver gehandhabt werden. So soll der sogenannte

„**A-Bogen**“, der eine Reihe von sensiblen Daten über den Gefangenen und seine Verwandten enthält, nur noch eingeschränkt zirkulieren. Bei Freigängern wird der Arbeitgeber des Gefangenen nicht mehr an die Pforte mitgeteilt. Generell soll beim Umbau der Pforten in den Justizvollzugsanstalten in Flensburg und Kiel durch bauliche Maßnahmen dafür gesorgt werden, daß die Offenbarung von Daten an Dritte vermieden wird.

Die Justizvollzugsanstalten sind in steigendem Maße auf die Mitarbeit Dritter, insbesondere **freiwilliger Helfer**, angewiesen. Künftig soll bei der Erstellung der Tagesordnung für Vollzugsplankonferenzen darauf geachtet werden, daß freiwillige Helfer keine Daten über Gefangene erhalten, für deren Betreuung sie nicht eingesetzt werden. In die Gefangenenpersonalakte wird ihnen keine Einsicht mehr gewährt. Die freiwilligen Helfer sollen verpflichtet werden, etwaige im Rahmen des Betreuungsauftrages entstandene Unterlagen mit Daten über den Gefangenen nach Erledigung des Betreuungsauftrages zu vernichten.

In einigen Punkten hat der Justizminister mitgeteilt, daß er den Forderungen/Empfehlungen des Landesbeauftragten nicht folgen möchte. So soll an der Ausgabe von **Paketmarken** festgehalten werden, die die Gefangenen für drei Pakete mit Nahrungs- und Genußmitteln zu verwenden haben. Wir hatten darin eine unnötige Offenbarung des Gefangenenstatus an Dritte gesehen.

Künftig sollen „abgängige“ Gefangenenstränke durch solche ersetzt werden, die auch ein **abschließbares Fach** haben. Dadurch soll es auch den Gefangenen möglich sein, ein Mindestmaß an **Privatsphäre** und an Sicherheit für die in den Zellen befindlichen Unterlagen zu erhalten. Allerdings soll es auch dann zulässig sein, dieses besonders abschließbare Behältnis in Abwesenheit des Gefangenen zu kontrollieren. Wir hatten statt dessen vorgeschlagen, dieses Behältnis nur im Beisein des Gefangenen zu durchsuchen, im übrigen aber Zellenrevisionen auch künftig in seiner Abwesenheit durchzuführen.

Der Justizminister hat mitgeteilt, daß er die Anforderung des Landesdatenschutzgesetzes, wonach jede **Datenübermittlung** zu **dokumentieren** ist, „angesichts der täglichen Flut eingehender Anfragen“ aus personellen Gründen in den Justizvollzugsanstalten nicht leisten könne. Dies wirft zunächst einmal ein Licht auf die Menge der offenbar durch die Justizvollzugsanstalten getätigten Datenübermittlungen. Aber selbst wenn der Umfang der Datenübermittlungen erheblich sein sollte, so sehen die klaren Regelungen des Landesdatenschutzgesetzes keine Ausnahme vor.

Zum überwiegenden Teil der Monita aus dem Prüfbericht hat der Justizminister bislang noch nicht Stellung genommen. Es geht dabei insbesondere um die zentralen Fragen des Umfangs der Datenerhebung und der Steuerung des sogenannten „A-Bogens“, der eine Reihe sensibler Daten über den Gefangenen

und über seine Verwandten enthält, innerhalb der Justizvollzugsanstalt. Auch zur künftigen Gestaltung, Handhabung und sicheren Aufbewahrung der **Gefangenenpersonalakten**, insbesondere auch der darin enthaltenen **Daten über Dritte**, hat der Justizminister bislang noch nicht Stellung genommen. Das gleiche gilt für Form und Inhalt des sogenannten „**AIDS-Hinweises**“, der nach unserer Auffassung in der gegenwärtigen Form rechtswidrig ist. Es bleibt zu hoffen, daß die weiteren notwendigen Konsequenzen für die Datenverarbeitung in den Justizvollzugsanstalten zügig gezogen werden.

4.3.4 Was Gefangene über ihr Wachpersonal in Erfahrung bringen konnten

Ein Gefangener verfügte über Kopien aus einer Ermittlungsakte gegen einen Bediensteten der Justizvollzugsanstalt. Die Herkunft der Unterlagen konnte nicht abschließend geklärt werden. Der Vorgang unterstreicht die Notwendigkeit, die Weitergabe von Daten oder ihre Nutzung für einen anderen Zweck zu dokumentieren.

Ausgerechnet einem Mitarbeiter einer schleswig-holsteinischen Justizvollzugsanstalt mußte es passieren, daß ihm ein Gefangener Kopien aus einer Strafermittlungsakte gegen ihn „zur Verfügung“ stellte, aus denen sich diverse hochsensible persönliche Informationen über ihn und dritte Personen ergaben. Nachdem er uns eingeschaltet hatte, nahmen wir zum Zweck der datenschutzrechtlichen Prüfung Einsicht in die Ermittlungsakte. Diese enthielt diverse **persönliche Daten** des Petenten, über seine familiären Verhältnisse, seine Ehefrau, Freunde, seine finanzielle Situation, einen vollständigen Grundbuchauszug über sein Grundvermögen, Informationen über seinen Pkw sowie über dritte Personen, die am Verfahren nicht beteiligt waren.

Es war zwar festzustellen, daß die Ermittlungsakte einem Anwalt zur Einsicht übersandt worden war. Von dort konnten aber aus bestimmten Gründen die Kopien, die der Gefangene in den Händen hatte, nicht stammen. Allerdings hatten sich aus den Aussagen der Zeugen in der Ermittlungsakte Anhaltspunkte für strafbare Handlungen anderer Personen ergeben. Die Kriminalpolizei ist diesen Anhaltspunkten nach Auskunft der Staatsanwaltschaft in der Form nachgegangen, daß sie **Kopien aus dieser Ermittlungsakte** fertigte und auf dieser Basis gesonderte Ermittlungsverfahren einleitete. Wenn in diese (durch die Kopien entstandenen) Akten Verteidiger Akteneinsicht genommen hatten, war nicht auszuschließen, daß auf diese Art und Weise Kopien aus der Ermittlungsakte in den Besitz von Gefangenen gekommen waren.

Allerdings war aus der ursprünglichen Ermittlungsakte nicht ersichtlich, gegen welche Personen neue Ermittlungsverfahren auf der Basis der gefertigten Kopien eingeleitet wurden. Es war auch **nicht dokumentiert**, welche Seiten aus der Akte in Kopie in andere Vorgänge übernommen worden waren. So

konnten Daten der geschilderten Art über den Petenten und von Unbeteiligten Eingang in Ermittlungsakten gegen andere Personen gefunden haben, ohne das dies nachvollziehbar war.

Eine weitere mögliche Datenquelle war die **unverschlossene Übersendung** der Ermittlungsakte an die Justizvollzugsanstalt, weil sie die Möglichkeit der Kenntnisnahme Dritter eröffnet hat. Dies haben wir gegenüber dem Generalstaatsanwalt kritisiert.

Wir haben überdies den Justizminister gebeten, sicherzustellen, daß künftig zur Vermeidung von Verstößen gegen das LDSG das **Fertigen von Kopien** zum Zwecke der Einleitung neuer Ermittlungsverfahren gegen andere Personen oder zu sonstigen Zwecken in der jeweiligen Ermittlungsakte **dokumentiert** wird. Der ebenfalls eingeschaltete Generalstaatsanwalt hielt es für geboten und „üblich“, daß beim Heraustrennen eines Ermittlungsverfahrens aus einem bestehenden, der neue Vorgang mit zu fertigenden Kopien aus den bereits bestehenden Akten eingeleitet wird. Allerdings geschehe dies nach seiner Auffassung nicht formlos, sondern stets mit einer Verfügung, die den Akt des Herausnehmens im abgebenden und einleitenden Vorgang erkennbar mache. Der Datenfluß bleibe somit rekonstruierbar. Vor diesem Hintergrund schien ihm das Anliegen des Datenschutzbeauftragten eine Selbstverständlichkeit zu sein. Die vorliegende Eingabe zeigt aber, daß in der Vergangenheit nicht in allen Fällen so verfahren wurde.

4.3.5 Mehr Datenschutz für Zeugen

Datenschutz für Zeugen nutzt auch der Strafverfolgung. Der Justizminister will in besonderen Fällen auf die Aufnahme der Zeugenanschrift in Anklageschriften und Strafbefehlsanträgen verzichten. Wir meinen, bei Strafbefehlsanträgen könnte die Zeugenanschrift stets entfallen.

Zu den wichtigsten Maßnahmen zur Effektivierung der Strafverfolgung zählt der **Zeugenschutz**. Datenschutz für Zeugen ist also alles andere als Täterschutz. Auch der Gesetzgeber hat inzwischen den Zeugenschutz verbessert und mehr Möglichkeiten eröffnet, daß ein Zeuge seine Anschrift oder seine Identität nicht offenbaren muß. In der Praxis ergeben sich aber immer wieder Abgrenzungsschwierigkeiten zwischen den schutzwürdigen Belangen von Zeugen und den legitimen Interessen einer effektiven Verteidigung.

Den Fall des Zeugen einer Schlägerei, der fürchtete, nunmehr selbst das Opfer des Schlägers zu werden und deshalb seine Privatanschrift nicht angeben wollte, haben wir zum Anlaß genommen, uns beim Justizminister für mehr Datenschutz für Zeugen einzusetzen. Per Erlaß hat er daraufhin den Gerichten und Staatsanwälten mitgeteilt, er habe keine Einwendungen, wenn „in besonderen Einzelfällen“ davon abgesehen werde, in die **Anklageschrift** oder den **Strafbefehlsantrag** die volle Zeugenanschrift aufzunehmen. Nach der jüngsten Novellie-

rung der Strafprozeßordnung besteht auch eine gesetzliche Grundlage, unter bestimmten Voraussetzungen von der Angabe der Privatadresse abzusehen. Es bleibt nach wie vor zu prüfen, ob nicht bei Strafbefehlsanträgen generell auf die Angabe der Zeugenanschrift verzichtet werden kann. In anderen Bundesländern wird bereits entsprechend verfahren. Dort geht man von der Überlegung aus, daß es in der großen Mehrzahl der Strafbefehlsverfahren nicht zu einem Einspruch und in der Folge zur mündlichen Verhandlung kommt. Deshalb brauche der Beschuldigte in diesem Verfahrensstadium die Privatanschrift von Zeugen noch nicht.

Um Zeugenschutz ging es auch in einem anderen Fall. In einer Ermittlungssache gegen Gefangene wegen Meuterei und Körperverletzung in der Frauenabteilung einer **Justizvollzugsanstalt** waren mehrere Vollzugsbeamte zur zeugenschaftlichen Vernehmung bei der Polizei vorgeladen worden. Die **Vorladung** erfolgte über die Anschrift der Justizvollzugsanstalt. Bei der Zeugenvernehmung mußten sie ihre **Privatanschrift** angeben, was zur Folge hatte, daß diese in der Anklageschrift in vollem Text erschien.

Einer der Betroffenen wandte sich an uns und berichtete, daß eine Gefangene in der Anstalt damit geprahlt habe, jetzt sei sie über die Privatanschriften des Aufsichtspersonals informiert. Dies verursachte bei dem Betroffenen und seinen Kolleginnen und Kollegen ein verständliches Unsicherheitsgefühl.

Die von uns eingeschaltete zuständige **Staatsanwaltschaft** kündigte an, sie werde künftig in Anklageschriften generell die Privatanschriften von Vollzugsbeamten nicht mehr nennen und statt dessen die **Dienstanschrift** verwenden. Die Maßnahme dürfte aber nur dann durchgreifenden Erfolg haben, wenn auch die Polizei bei ihren Vernehmungen entsprechend verfährt. Wir haben den Innenminister gebeten, für eine solche Verfahrensweise Sorge zu tragen. Dieser teilte inzwischen mit, er habe das Kriminalpolizeiamt gebeten, entsprechend zu verfahren. Künftig solle bei polizeilichen Vernehmungen **generell** auf die Nennung der **Privatanschrift verzichtet** werden, wenn es sich um Zeugen handele, bei denen im Rahmen der Erfüllung ihrer Dienstgeschäfte die Besorgnis einer Gefährdung bestehe.

4.3.6 Risiken bei der Genomanalyse in Strafverfahren

Eine einwandfreie gesetzliche Grundlage für Genomanalysen im Strafverfahren fehlt nach wie vor. Auch die schleswig-holsteinische Polizei soll künftig für die Durchführung von Genomanalysen ausgerüstet werden. Die Analysen sollen sich aber nur auf den „nichtcodierenden“ Bereich der Genome beziehen.

Der Gesetzentwurf zur Einführung des sogenannten genetischen Fingerabdrucks in das Strafverfahren ist auch im vergangenen Jahr nicht verabschiedet worden. Gleichwohl sind

die technischen Möglichkeiten der Polizei zur Durchführung von **Genomanalysen** weiter verbessert worden. Auch in Schleswig-Holstein ist für 1993 geplant, Genomanalysen in den Bereich der Kriminaltechnik des Kriminalpolizeiamtes einzuführen.

Wir sind nach wie vor der Auffassung (vgl. 12. TB, S. 48), daß die **Strafprozeßordnung** in ihrer gegenwärtigen Form als Rechtsgrundlage für Genomanalysen **nicht ausreicht**. Das entscheidende Risiko, das aus datenschutzrechtlicher Sicht bei Genomanalysen besteht, liegt nicht in der Entnahme der für die Durchführung der Analyse notwendigen Blutproben oder anderen körperlichen Stoffe. Problematisch ist vielmehr die Möglichkeit, daß im Rahmen der Genomanalyse über die Identität hinaus Feststellungen zu Erbanlagen, persönlichen Eigenheiten, Veranlagungen zu bestimmten Krankheiten etc. getroffen werden. Diese Risiken für das allgemeine Persönlichkeitsrecht sind in der Strafprozeßordnung nicht hinreichend behandelt und sollen erst durch den erwähnten Gesetzentwurf berücksichtigt werden.

Gegen die Einrichtung von **Genomanalyse-Verfahren** in **Schleswig-Holstein** vor Verabschiedung der notwendigen gesetzlichen Grundlagen bestünden Bedenken, wenn nicht sichergestellt wäre, daß sich die Genomanalyse ausschließlich auf die **Feststellung der Identität beschränken** wird. Auf entsprechende Nachfrage teilte der Innenminister mit, daß im Rahmen der geplanten Maßnahmen lediglich Analysen im sog. **nichtcodierenden Bereich** der Genome durchgeführt werden sollen. Dementsprechend könnten auch nur Identitätsfeststellungen und nicht weitergehende Persönlichkeitsanalysen durchgeführt werden.

Inzwischen hat die **Polizei** öffentlich Klage geführt, Politiker „blockierten“ ein „sicheres Beweismittel“. Gemeint war damit aber nicht die noch fehlende Rechtsgrundlage, sondern das Fehlen von ausreichend geschultem Personal, um in Schleswig-Holstein mit der Durchführung von Genomanalysen beginnen zu können. Beim Bundeskriminalamt müsse man ein Jahr auf Ergebnisse warten. Solange könne man Tatverdächtige nicht in Untersuchungshaft halten.

Bei solcher Argumentation drängt sich die Frage auf, wie die Polizei vor Entdeckung der Genomanalyse, die erst vor wenigen Jahren erfolgte, ermittelt hat. Die Gerichte, die bislang die Genomanalyse nur zögernd zugelassen haben, stellen darauf ab, daß eine Verurteilung nicht allein auf das Ergebnis der Genomanalyse gestützt werden darf. Es sei nur ein – wenn auch relativ sicheres – Beweismittel neben anderen. Die Polizei kommt also nicht umhin, auch nach Einführung der Genomanalyse in Schleswig-Holstein auch weiterhin parallel zu ermitteln.

4.3.7 **Mitteilungen in Strafsachen: Gesetz läßt weiter auf sich warten**

Das Justizmitteilungsgesetz ist noch nicht verabschiedet. Die Datenübermittlungen nach der Verwaltungsvorschrift „Mitteilungen in Strafsachen“ laufen weiter. Die Praxis konnte im Berichtsjahr geringfügig verbessert werden.

Das seit Jahren angekündigte **Justizmitteilungsgesetz** ist auch im Berichtszeitraum nicht verabschiedet worden. Nach wie vor werden aber Datenübermittlungen über Strafverfahren nach der Verwaltungsvorschrift „Mitteilungen in Strafsachen“ (MiStra) vorgenommen. Wir bemühen uns seit langem, zumindest in der praktischen Anwendung der MiStra datenschutzrechtliche Verbesserungen zu erreichen.

Der **Justizminister** hat im Berichtsjahr mitgeteilt, daß er die Staatsanwaltschaften um Berücksichtigung folgender Gesichtspunkte gebeten habe:

- Der jeweilige **Empfänger** soll darauf **hingewiesen** werden, daß eine Verwendung der in der Mitteilung enthaltenen Daten nur für den Zweck zulässig ist, für den sie übermittelt worden sind. Im Falle der Zweckerreichung sind sie zu vernichten.
- Der Beschuldigte ist zeitgleich mit der Veranlassung der Mitteilung selbst zu **benachrichtigen**.

Darüber hinaus gab der Justizminister zu erwägen, ob die Mitteilung nicht erst nach Zustellung der Anklage oder des Strafbefehls erfolgen könne. In der Anklageschrift bzw. im Strafbefehlsantrag könne dann bereits auf die beabsichtigte Mitteilung hingewiesen werden. Diesen Vorschlag haben wir unterstützt, weil in diesen Fällen dann auch unserer Forderung Rechnung getragen wäre, daß der **Betroffene vor der Mitteilung** Kenntnis erhält. Er kann sich dann rechtzeitig darauf einstellen und seinem Dienstherrn eine Schutzschrift oder eine andere Form der „Gegendarstellung“ an die Hand geben.

4.3.8 **Datenschutzrechtliche Probleme beim Grundbuch**

Auch der Justizminister bejaht nunmehr die Notwendigkeit, Einsichtnahmen in das Grundbuch zu protokollieren. Damit kann künftig nachvollzogen werden, wer wann Einsicht in das Grundbuch genommen hat.

In den vergangenen Jahren wurde mehrfach über unsere Forderung berichtet, **Einsichtnahmen** in das und Abschriften aus dem Grundbuch zu **dokumentieren** (vgl. 12. TB, S. 53). Dabei gehen wir davon aus, daß es ein erhebliches berechtigtes Interesse von Grundstückseigentümern gibt, nachvollziehen zu können, wer sich für ihre Eigentums-, und im Hinblick auf ggf. eingetragene Grundpfandrechte, finanziellen Verhältnisse interessiert. Nunmehr ergibt sich auch aus dem LDSG die Verpflichtung, jede **Datenübermittlung** zu **protokollieren**. Wir

haben den Justizminister Anfang des Jahres gebeten, seinen bislang ablehnenden Standpunkt noch einmal zu überprüfen. Auch er ist jetzt der Auffassung, daß die Einsichtnahme in das Grundbuch protokolliert werden muß. Er ist derzeit dabei, noch offenstehende praktische Fragen mit den Gerichten zu klären.

Auch im Berichtsjahr gab es wiederholt Eingaben, die sich mit datenschutzrechtlichen Fragen im Zusammenhang mit dem Grundbuch und Grundbuchauskünften befaßten. Ein Petent besaß z.B. einen **Miteigentumsanteil** an einem Grundstück. Ein anderer Miteigentümer erhielt einen Grundbuchauszug, der sämtliche Miteigentumsanteile einschließlich der jeweiligen Grundstücksbelastungen enthielt. Wir nahmen dies zum Anlaß, den Justizminister erneut zu bitten, sich für eine datenschutzgerechte Überarbeitung der entsprechenden Vorschriften der Grundbuchordnung einzusetzen. Der Justizminister teilte mit, daß auf Bundesebene bereits eine Änderung der Grundbuchordnung in Vorbereitung sei. Bis dahin solle in verstärktem Maße von der Möglichkeit Gebrauch gemacht werden, Miteigentumsanteile nur bei dem Hauptgrundstück und nicht mit einem eigenen Grundbuchblatt zu buchen. Die Grundbuchordnung läßt eine entsprechende Fallgestaltung zu. In diesem Falle kann es dann nicht mehr zu Auskünften der vom Petenten geschilderten Art kommen. Der Justizminister hat in einem Erlaß an alle Grundbuchämter darauf hingewiesen und gebeten, den datenschutzrechtlichen Belangen auf diese Weise gerecht zu werden.

4.4 **Steuerverwaltung**

4.4.1 **Was hat der Name des Hypothekengläubigers mit der Höhe eines Einheitswertes zu tun?**

Die Behörden im Lande neigen nach wie vor dazu, mittels „hausgemachter“ Vordrucke zu viele Daten zu erheben. Nach unserer Intervention zog die Finanzministerin einen zu weit gefaßten Vordruck zurück.

Einheitswerte werden von Finanzämtern ermittelt, um den **steuerlichen Wert von Grundstücken** bei der Festsetzung der Grundsteuer, der Gewerbesteuer, der Vermögenssteuer, der Einkommensteuer usw. zu berücksichtigen. Es handelt sich dabei um „künstliche“ Werte, die z.B. bei Einfamilienhäusern aus dem Mietwert nach den Wertverhältnissen von 1964 abgeleitet werden. Deshalb war ein Steuerpflichtiger erstaunt, daß man von ihm in einem Vordruck der als „Grundstücksbeschreibung“ bezeichnet war, auch Angaben über die Höhe der Fremdfinanzierung, die Namen der Geldgeber sowie die Höhe der Zinsen und der Tilgungsraten abverlangte. Die Nachfrage beim Finanzamt, was denn z.B. die **Namen der Hypothekengläubiger** mit der Höhe des Einheitswertes zu tun hätten, führten zwar zu einer Belehrung über das Recht der Einheitsbewertung im allgemeinen, nicht aber zu einer kon-

kreten Antwort auf die gestellte Frage. Es wurde schlicht festgestellt, daß die Angaben erforderlich seien.

Auch uns gelang es nicht, die Oberfinanzdirektion als die nächst „höhere“ Instanz dazu zu bewegen, besagte Erforderlichkeit zu begründen. Man beharrte darauf, daß die Angaben über die Finanzierung der Immobilie für die Feststellung des Einheitswerts „sachdienlich“ seien.

Als wir diese Form der Datenerhebung daraufhin förmlich beanstandeten, schaltete sich die **Finanzministerin** ein. Nach Befragung der Finanzministerien der anderen Bundesländer wurde folgende Entscheidung getroffen: „Der Vordruck wird zukünftig entsprechend überarbeitet.“ Statt detaillierte Finanzierungspläne abzufordern, wird richtigerweise nur noch die Frage gestellt, ob der Wohnraum mit öffentlichen Mitteln oder anderen zinsverbilligten Darlehen gefördert worden ist.

4.4.2 Datensicherheit für Akten und sonstige Unterlagen

Der Zugang zu EDV-Dateien ist nicht selten besser gesichert als die Akten und Schriftstücke, deren Inhalt ohne Hilfe von Programmen von jedermann zur Kenntnis genommen werden kann.

Die Begrenzung des Anwendungsbereiches des alten Landesdatenschutzgesetzes auf Karteien und EDV-Dateien haben wir stets in einer Hinsicht ganz besonders bedauert: In den vergangenen Jahren haben wir immer wieder festgestellt, daß die Maßnahmen zur **sicheren Verwahrung** von **Akten** und sonstigen **Verwaltungsunterlagen** mit personenbezogenem Inhalt sehr viel mehr zu wünschen übrig ließen als die technischen und organisatorischen Maßnahmen im Rahmen von automatisierten Verfahren. Wir haben dies zwar stets kritisiert (vgl. z.B. 14. TB, S. 81), haben aber auf formelle Beanstandungen verzichtet, um uns nicht dem Vorwurf der Kompetenzüberschreitung auszusetzen.

Diese Zurückhaltung ist nun nicht mehr notwendig, da das neue Landesdatenschutzgesetz grundsätzlich auf alle personenbezogenen Daten bei Behörden Anwendung findet. Dem in diesem Bereich offensichtlich bestehenden **Nachholbedarf** soll durch **verstärkte Kontrollen** Rechnung getragen werden. Dabei erscheint es folgerichtig, sich zunächst mit solchen Unterlagen zu befassen, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen.

Wenn der Gesetzgeber für bestimmte Datenbestände besonders strenge Geheimhaltungsbestimmungen formuliert hat und ihre Durchbrechung auf der Grundlage spezieller Straftatbestände ahndet, so muß die Verwaltung diesem Umstand durch **effektivere Sicherungsmaßnahmen** Rechnung tragen, als sie bei „normalen“ Verwaltungsdaten erforderlich und angemessen sind. Werden Patientendaten, Sozialdaten, Statistikdaten, Post- und Fernmeldedaten usw. verarbeitet, haben die Behörden ein erhöhtes Maß an Sicherheit zu gewährleisten.

Das gilt im übrigen auch für Datenbestände, deren unbefugte Offenbarung aus anderen Gründen unbedingt verhindert werden muß (Daten, die einer Behörde von einem Bürger freiwillig für einen ganz bestimmten Zweck zur Verfügung gestellt wurden, Vertragsdaten, noch nicht verifizierte Verdachtsmomente bei Sicherheitsbehörden und dergl.).

Zu den besonders „sensiblen“ Datenbeständen gehören auch die **Steuerakten** in den Finanzämtern, deren Inhalt dem Steuergeheimnis unterliegt. Hierbei handelt es sich um einen wahrlich riesigen Bestand. Auf 20 Finanzämter verteilt dürften mehr Steuerakten der verschiedensten Art (von Einkommenssteuer- und Lohnsteuerjahresausgleichsakten über Kraftfahrzeugsteuerakten und Einheitswertakten bis hin zu Erbschafts- und Schenkungssteuerakten) lagern, als Schleswig-Holstein überhaupt Einwohner hat, also in einer Größenordnung von mehr als 2,5 Millionen.

Vor Beginn unserer **Stichprobenkontrolle** in einigen Finanzämtern, haben wir uns zunächst von der Oberfinanzdirektion darlegen lassen, zu welchen Datensicherungsmaßnahmen die einzelnen Finanzämter nach der „Erlaßlage“ verpflichtet sind. Es ergab sich folgendes Bild:

Die einschlägige Verwaltungsanweisung behandelt dieses Thema lediglich mit zwei Sätzen. Die Akten sind danach durch „geeignete“ Maßnahmen – insbesondere außerhalb der Dienststunden – vor einer Einsichtnahme durch Unbefugte zu schützen; werden Akten „außerhalb der regelmäßigen Bearbeitung ausgegeben“, ist der Empfänger zu vermerken und die Rückgabe zu überwachen. Als geeignete Maßnahmen sieht die Oberfinanzdirektion „z.B.“ das Verschließen von Schränken und Diensträumen und das Vernichten von Schriftgut und Papierabfällen an.

Ebenso spartanisch wie die Anweisungen der Oberfinanzdirektion sind die **Maßnahmen**, die die geprüften **Finanzämter** in bezug auf die Sicherung ihrer Aktenbestände getroffen haben.

- Die in den jeweiligen **Hausordnungen** enthaltenen Regelungen sind häufig in sich **nicht schlüssig**. Einerseits sollten Akten und Schriftstücke so aufbewahrt werden, daß sie Unbefugten nicht zugänglich sind, andererseits ist die Lagerung von Unterlagen auf offenen Aktenböcken ausdrücklich zugelassen.
- Bei allen geprüften Finanzämtern fehlt es an einer ausreichenden Zahl von verschließbaren **Schränken**. Auch wenn sie vorhanden sind, bleiben sie häufig über Nacht **unverschlossen**. In einem Fall einfach deshalb, weil die Schlüssel verloren gegangen waren.
- Die **Büroräume** werden nicht selten auch während der Geschäftszeiten bei Abwesenheit der Mitarbeiter **unverschlossen gelassen**. Unser Prüfungsbeamter hatte bei einer Stichprobe hinreichend Zeit, sich in einer Aktenverwaltungsstelle unbeaufsichtigt umzusehen.

- In Altarchiven fehlen ausreichende Sicherheitsmaßnahmen.
- **Aktenherausgaben** an Außendienstmitarbeiter werden **nicht registriert**. Es gibt keine Anweisungen für diese Mitarbeiter, wie Steuerakten in ihrer Privatwohnung und während der Außendiensttätigkeit zu sichern sind.
- Der **Zugang** zu den **Diensträumen** ist trotz gleicher Ausgangslage sehr unterschiedlich geregelt. Während ein Finanzamt ein dienststellenbezogenes Sicherheitsschließsystem realisiert hat, sind in anderen Finanzämtern keine besonderen Sicherheitsvorkehrungen getroffen worden.

Wir haben diese Mängel beanstandet und die Oberfinanzdirektion aufgefordert, als weisungsbefugte Aufsichtsbehörde durch entsprechende Regelungen dafür zu sorgen, daß in allen Finanzämtern des Landes ausreichende Sicherungsmaßnahmen getroffen werden.

4.5 Wirtschaft, Technik und Verkehr

„Schwarze Liste“ über Heimarbeitgeber

Bei der Vergabe von Heimarbeit können unseriöse Arbeitgeber den Heimarbeitern Nachteile oder Schäden zufügen. Für die Erfassung solcher Stellen in einer „schwarzen Liste“ besteht für Landesbehörden keine ausreichende Rechtsgrundlage.

Nach dem Heimarbeitsgesetz ist der Entgeltschutz der Heimarbeit durch sogenannte **Entgeltüberwachungsstellen** der Länder zu kontrollieren. Die dabei anfallenden Erkenntnisse über unseriöse Praktiken bei der Vergabe von Heimarbeit werden regelmäßig dem bayerischen Staatsministerium für Arbeit, Familie und Sozialordnung mitgeteilt, dort zusammengefaßt und in die „Liste nicht empfehlenswerter Auftraggeber“ aufgenommen. Anschließend wird die Liste bundesweit an die jeweils zuständigen Stellen übersandt, die ihrerseits dann im Einzelfall aus dieser Liste auch Auskünfte an Heimarbeit-suchende erteilen.

So löblich die Absicht ist, unseriösen Heimarbeitgebern das Handwerk zu legen, so untauglich ist die Liste in dieser Form. Nicht nur, daß eine ausreichende **Rechtsgrundlage fehlt**. Darüber hinaus handelt es sich bei den einzelnen Angaben in der Liste um Sachverhalte, die gegenüber dem Betroffenen nicht rechtskräftig festgestellt wurden. Zum Teil wird mit Behauptungen gearbeitet, die sich allein auf die Auskunft einzelner Arbeitnehmer stützen, ohne daß die Angaben in einem Verwaltungsverfahren überprüft worden sind. Die Betroffenen werden über diese Feststellungen weder unterrichtet, noch haben sie Kenntnis von der Aufnahme in die Liste.

Unter diesen Umständen konnten wir bei unserer datenschutzrechtlichen Prüfung nur zu dem Ergebnis kommen, daß zumindest in Schleswig-Holstein eine weitere Verwendung die-

ser Daten gegen geltendes Datenschutzrecht verstößt. Soll die Zuverlässigkeit der Heimarbeitgeber, ähnlich wie im Gewerbebereich, effektiv überwacht werden, müssen entsprechende Regelungen für ein rechtstaatliches Verfahren im Heimarbeitsgesetz getroffen werden.

4.6 Sozial- und Gesundheitswesen

4.6.1 Sozialwesen

4.6.1.1 Datenerhebung beim Betroffenen oder Amtsermittlung?

Angaben für soziale Leistungen sind zunächst vom Leistungsempfänger beizubringen oder bei ihm zu erfragen. Erst wenn er solche Angaben nicht macht oder Zweifel an ihrer Richtigkeit bestehen, kann von Amts wegen ermittelt oder wegen fehlender Mitwirkung des Betroffenen eine Leistung abgelehnt werden.

Es wird immer wieder gefragt, ob Ämter, bevor sie soziale Leistungen gewähren, sofort von Amts wegen die Leistungsvoraussetzungen klären und dabei auch Auskünfte von Dritten wie z.B. Arbeitgebern oder Vermietern einholen dürfen, oder ob sie zunächst den Antragsteller um Informationen bitten müssen. Beschwerden sich die betroffenen Bürger hierüber, wird stets auf den Amtsermittlungsgrundsatz oder „**Untersuchungsgrundsatz**“, wie es im Sozialgesetzbuch (SGB) heißt, verwiesen.

Zwei Fälle aus der Praxis machen das deutlich:

- Ein Handelsvertreter, der als Bezirkskommissar für eine Versicherung tätig ist, wurde Vater. Er beantragte beim Versorgungsamt **Erziehungsgeld** für sich für den Zeitraum von einem Jahr. Das Versorgungsamt wandte sich unmittelbar an die Versicherung, für die der Vater tätig ist, mit der Frage, ob sich die mit der Funktion eines Bezirkskommissars verbundenen Aufgaben auf eine Arbeitszeit von maximal 19 Wochenstunden reduzieren lassen. Nur dann besteht ein Anspruch auf Erziehungsgeld. Arbeitnehmer müssen die kurzzeitige Beschäftigung durch eine Arbeitsbescheinigung nachweisen, Selbständige müssen glaubhaft machen, daß sie zur Betreuung des Kindes ihre Tätigkeit entsprechend einschränken. Der Handelsvertreter befürchtete berufliche Schwierigkeiten und beschwerte sich über das eigenmächtige Vorgehen des Versorgungsamtes.
- Dem zuständigen Beamten eines Sozialamtes war aufgefallen, daß ein Empfänger von **Sozialhilfe** (Hilfe zum Lebensunterhalt) einen Mercedes 250 SE fuhr. Er nahm sich vor, den Betroffenen beim nächsten Besuch zu befragen, ob der Pkw ggf. als verwertbares Vermögen einzusetzen sei. Durch Zufall hatte der Beamte einige Tage später in seiner Eigenschaft als nebenamtlicher Versicherungsvertreter für dasselbe Fahrzeug einen Versicherungsantrag aufzunehmen. Als

der Betroffene wieder im Sozialamt erschien, fragte ihn der Beamte nach den Eigentumsverhältnissen. Als der Sozialhilfeempfänger bestritt, Eigentümer zu sein, hielt ihm der Beamte vor, daß ihm als nebenamtlichem Mitarbeiter einer Versicherung ein Versicherungsantrag für diesen Wagen auf seinen Namen vorliege. Der Sozialhilfeempfänger erklärte, das Fahrzeug gehöre seiner Freundin, die in einer anderen Stadt lebe und sämtliche Unkosten für den Pkw bezahle. Der Wagen solle nur aus versicherungstechnischen Gründen auf seinen Namen zugelassen werden. Er beschwerte sich darüber, daß der Beamte im Sozialamt die ihm aus seiner Versicherungstätigkeit bekannten Daten für seine amtliche Tätigkeit genutzt habe.

Im **ersten Fall** war es nach unserer Auffassung nicht zulässig, unmittelbar die Versicherung zu befragen. Der Vater hätte vielmehr unter Hinweis auf seine Mitwirkungspflicht aufgefordert werden müssen, den Sachverhalt schlüssig darzulegen und ggf. auch entsprechende Nachweise beizubringen. Selbst wenn dann weiterhin Unklarheit bestanden hätte, ob ein Anspruch auf Erziehungsgeld bestand, wäre die Einschaltung der Versicherung und die damit erfolgte Offenbarung von Sozialdaten unzulässig. Bei fortbestehenden Zweifeln hätte der Antrag auf Gewährung von Erziehungsgeld abgelehnt werden müssen. Es wäre Sache des Antragstellers gewesen, im weiteren Verfahren nachzuweisen, daß er tatsächlich nur halbtags tätig ist. Die Übermittlung der Sozialdaten an die Versicherung war eine unbefugte Offenbarung und somit ein Verstoß gegen das Sozialgeheimnis, der förmlich beanstandet werden mußte.

Bei dem **zweiten Fall** war davon auszugehen, daß dem Mitarbeiter im Sozialamt bereits aus seiner amtlichen Tätigkeit – er sah den Sozialhilfeempfänger wegfahren – bekannt war, daß dieser einen wertvollen Pkw fuhr. Zur Klärung der Einkommens- und Vermögensverhältnisse wäre er berechtigt gewesen, die Vorlage des Kfz-Scheines zu verlangen. Bei Nichtvorlage wären dann auch weitere Ermittlungen von Amts wegen – allerdings kaum bei der Versicherung – zulässig gewesen. Daß an die Stelle amtlicher Ermittlungen die Verwertung privater Zusatzkenntnisse trat, macht das eigentliche Problem aus. In der Regel dürfte nämlich die Verwertung solcher Informationen in Verwaltungsverfahren eine Vertragsverletzung des Mitarbeiters bedeuten.

4.6.1.2 Grenzen der Datenerhebung durch das Sozialamt

Wird Sozialhilfe gezahlt, so kann das Sozialamt Unterhaltsansprüche des Empfängers auf sich überleiten. Dazu darf es Informationen über Einkommen und Vermögen des Unterhaltspflichtigen erheben. Ein Anspruch auf entsprechende Angaben über dessen nicht unterhaltspflichtigen Ehegatten besteht jedoch nicht.

Zahlt ein Sozialamt Sozialhilfe, so leitet es Unterhaltsansprüche des Hilfeempfängers gegen seine Verwandten auf sich

über. Der unterhaltspflichtige Angehörige hat zu diesem Zweck **Angaben** über seine **wirtschaftlichen Verhältnisse** zu machen. Immer wieder beschwerten sich Unterhaltspflichtige darüber, daß von ihnen auch Angaben über das Einkommen und Vermögen ihrer **Ehegatten** verlangt werden, auch wenn diese nicht unterhaltspflichtig sind.

Wir vertreten die Auffassung, daß das Bundessozialhilfegesetz keine Befugnis für Datenerhebungen über das Einkommen und Vermögen nicht unterhaltspflichtiger Angehöriger enthält. Es kann allerdings im Einzelfall durchaus im Interesse des Unterhaltspflichtigen liegen, solche Angaben zu machen. Dies wird dann der Fall sein, wenn der nicht Unterhaltspflichtige kein eigenes oder nur ein geringes Einkommen oder Vermögen hat und der Unterhaltspflichtige auch ihm Unterhalt gewähren muß. Dies darf jedoch nur mit dem **Einverständnis** des nicht unterhaltspflichtigen Angehörigen geschehen und ist durch seine Unterschrift auf dem Fragebogen zu dokumentieren.

4.6.1.3 Keine Amtshilfe für die Telekom

Nach der Postreform nimmt die Telekom gegenüber den Kunden keine Aufgaben der öffentlichen Verwaltung wahr. Ein Anspruch auf Amtshilfe nach dem Sozialgesetzbuch besteht daher nicht mehr.

Daß die Postreform auch Auswirkungen im Bereich des Sozialgesetzbuches hat, kann man nicht ohne weiteres erwarten. Doch ergaben sich für einige **Krankenkassen** Probleme. Für sie war es fraglich, ob nach der Neuordnung der Deutschen Bundespost die **Telekom** Anspruch auf Auskünfte im Rahmen der **Amtshilfe** habe. Wie früher baten die Fernmeldeämter unter Bezugnahme auf die Amtshilfavorschriften des SGB X nämlich um Auskunft über Beschäftigungsverhältnisse von Kunden der Telekom. Die Angaben sollten der Ermittlung des derzeitigen Arbeitgebers für Zwecke der Vollstreckung dienen.

Die Telekom ist zwar nach wie vor Teil der bundeseigenen Verwaltung, uns wurde jedoch auf Nachfrage bestätigt, daß sie gegenüber ihren Kunden nur **privatrechtlich tätig** ist. Für die Anwendung der Amtshilfavorschriften des SGB X wäre jedoch Voraussetzung, daß die Telekom gegenüber ihren Kunden hoheitlich tätig wird. Die betroffenen **Krankenkassen** wurden darauf hingewiesen, daß aus Amtshilfavorschriften keine Offenbarungsbefugnis für solche Auskünfte hergeleitet werden kann, die zur Beitreibung privatrechtlicher Forderungen der Telekom verwendet werden sollen.

4.6.1.4 Stichprobenprüfungen in Sozialämtern

Die Akten der geprüften Sozialämter wurden durchweg sorgfältig geführt. Dennoch zeigte die Aktenführung einige grundsätzliche Rechtsprobleme auf.

Im Rahmen von **Stichprobenprüfungen** bei vier Sozialämtern haben wir Akten über die Gewährung von Hilfe zum Lebensunterhalt, Hilfe zur Pflege, Eingliederungshilfe und Heimunterbringung gezielt auf drei Fragestellungen hin durchgesehen:

- Gab es unbefugte Datenerhebungen bei Dritten?
- Gab es unbefugte Offenbarungen von Sozialdaten an Dritte und
- wurden bei Datenerhebungen über Unterhaltspflichtige im Zusammenhang mit Überleitungsanzeigen nach den §§ 90, 91 Bundessozialhilfegesetz (BSHG) auch unbefugt Daten über deren nicht unterhaltsverpflichtete Ehegatten erhoben?

Dabei fiel auf, daß offensichtlich von allen vier geprüften Sozialämtern beim Zuzug solcher Sozialhilfeempfänger, die bereits am alten Wohnort Sozialleistungen erhalten haben, die **frühere Sozialhilfeakte** zur **Einsichtnahme** und Fertigung von Kopien angefordert wird. Dies geschieht nur teilweise mit Einwilligung der betroffenen Antragsteller. In der Regel werden die letzten maßgeblichen Bescheide des Sozialamtes und Nachweise wie Rentenbescheid, Verdienstbescheinigung und Mietvertrag kopiert, bei Asylbewerbern auch die Zuweisungsbescheide. Auf unsere Frage, warum die Akten ohne Einschränkung angefordert werden, wurde mehr oder weniger übereinstimmend erklärt, man brauche die Akten, um die genannten Nachweise zu erhalten und um z.B. festzustellen, wann und in welcher Höhe die letzten Bekleidungsbeihilfen u.ä. bewilligt worden seien.

Nach der Rechtslage sind die Sozialämter nur berechtigt, die für die Bearbeitung der jeweiligen Hilfe **erforderlichen Daten** zu erheben. Dieser Maßstab gilt auch für Datenanforderungen bei anderen Behörden. Da die geprüften Sozialämter nur die aktuellen Unterlagen aus den angeforderten Akten kopiert haben, sind in der Mehrzahl der Fälle mit den vollständigen Akten auch nicht erforderliche Daten an das neu zuständige Sozialamt übermittelt worden. Die benötigten Informationen betrafen durchweg nur die letzten Zeiträume einer Sozialhilfegewährung oder bestimmte Arten der Hilfeleistung. Sie hätten ohne wesentlichen Aufwand von früheren Akteninhalten **getrennt** oder in Form einer Auskunft dem anfragenden Sozialamt zur Verfügung gestellt werden können.

Kritisch ist jedoch nicht nur der Umfang der angeforderten Daten – die gesamte Akte –, sondern es stellt sich grundsätzlich die Frage, ob solche unmittelbaren Auskunftersuchen bei der früher zuständigen Behörde erforderlich sind. **Daten** sind, auch wenn es Sozialhilfeempfänger betrifft, grundsätzlich zunächst **beim Betroffenen** zu **erheben**. Ein Auskunftersuchen bei Dritten kann allenfalls in bezug auf die bereits erwähnten Bekleidungsbeihilfen oder ggf. spezielle Beihilfen im Rahmen der Eingliederungshilfe erforderlich sein, wenn Zweifel an den Angaben der Betroffenen bestehen. Wir halten daher die routinemäßige Anforderung der vollständigen So-

zialhilfeakte beim früher zuständigen Sozialamt ohne Einwilligung der Betroffenen im Grundsatz für unzulässig.

Aber auch mit **Einwilligung** ist die Anforderung der vollständigen Akte nicht ohne weiteres zulässig. Ein Bürger, der einen Antrag in einem Sozialamt stellt, möchte eine Leistung des Staates erhalten und wird daher, wenn es von ihm verlangt wird, „notgedrungen“ auch eine Unterschrift unter eine generelle Einverständniserklärung geben. Deshalb dürfen die Behörden sich von vornherein eine Einwilligung zur Beiziehung von Unterlagen nur im erforderlichen Umfang geben lassen.

Weiter war den Sozialakten zu entnehmen, daß es verhältnismäßig häufig zu Kontakten oder zu **Schriftwechsel** des Sozialamtes **mit Dritten** kommt, ohne daß eine vorherige Beteiligung des Antragstellers erkennbar wird. Als Beispiele seien hier genannt:

- Befragung eines Autohauses über den Kaufpreis des Pkw eines Sozialhilfeempfängers,
- Schriftwechsel mit einer Wohnungsbaugesellschaft über Mietrückstände und den Neuabschluß eines Mietvertrages,
- Kontakte mit Rechtsanwälten in Scheidungs- und Erbschaftssachen,
- Kontakte mit Bestattungsunternehmen,
- Schriftwechsel mit Alten- und Pflegeheimen und
- Stellungnahmen anderer Ämter (Ordnungsamt, Steueramt) der eigenen Verwaltung.

Dabei werden sowohl Daten erhoben als notgedrungen auch die Tatsache des **Sozialhilfebezugs offenbart**. Wir haben in den genannten Fällen mehrheitlich in den Akten keine Einverständniserklärung der betroffenen Antragsteller zu diesen Datenerhebungen und Offenbarungen an Dritte gefunden, noch Hinweise darüber, daß die Betroffenen darüber informiert worden waren.

Auch wenn man bei der Mehrzahl der Fälle davon ausgehen kann, daß das Handeln des Sozialamtes im Ergebnis für den Betroffenen nicht von Nachteil war, verstößt das Verfahren ohne schriftliche Einwilligung gegen den Sozialdatenschutz. Auch Sozialdaten sind zunächst immer beim Betroffenen zu erheben und ihre Offenbarung darf nur in den im Sozialgesetzbuch genannten Fällen erfolgen. Die Sozialämter müssen, wenn sie selbst ermitteln oder für den Sozialhilfeempfänger Angelegenheiten klären wollen, zunächst das **schriftliche Einverständnis** der Betroffenen einholen. Im Ausnahmefall – bei Vorliegen besonderer Umstände – kann auch das mündliche Einverständnis genügen. Wichtig ist jedoch, daß auch das mündlich eingeholte Einverständnis schriftlich in den Akten dokumentiert wird. Sinn dieser Regelung ist die Garantie des informationellen Selbstbestimmungsrechts auch für Sozialhilfeempfänger, die nicht wie Entmündigte behandelt werden dürfen.

In diesem Zusammenhang ist auch die Offenbarung und die Erhebung von Sozialdaten bei der Anmeldung und Durchsetzung von **Erstattungsansprüchen** nach dem Sozialgesetzbuch X zu erwähnen. Hier findet in der Regel Schrift- und Telefonverkehr u.a. mit dem Arbeitsamt, der Landesversicherungsanstalt, der Bundesversicherungsanstalt für Angestellte und dem Versorgungsamt statt. Dies ist, soweit es sich um die Anmeldung und Abwicklung der Erstattungsansprüche handelt, auch korrekt. Auch soweit es in diesem Zusammenhang zur Offenbarung von Sozialdaten kommt, ist diese nach SGB X zulässig.

Allerdings wurde im Rahmen der Prüfung festgestellt, daß es auch unabhängig von der Geltendmachung von Erstattungsansprüchen zu der Anforderung von Rentenbescheiden sowie anderen Anfragen oder Mitteilungen wie z.B. der Übermittlung von Berichten des Arbeitsamtes nach Auslaufen der dortigen Förderung kommt. Soweit dies über den Erstattungs-zweck hinausgeht, hat nach den Vorschriften des SGB X die Erhebung beim Betroffenen zu erfolgen. Nur im Ausnahmefall oder mit schriftlicher Einwilligung des Betroffenen kann die Datenerhebung unmittelbar bei den genannten Institutionen in Frage kommen.

4.6.2 Gesundheitswesen

4.6.2.1 Abgleich von Betäubungsmittelrezepten eines Gesundheitsamtsbezirks

Rezepte zum Bezug von Betäubungsmitteln dürfen vom Gesundheitsamt überprüft werden. Eine patientenbezogene Auswertung aller Betäubungsmittelrezepte eines Gesundheitsamtsbezirks zur Kontrolle von Betäubungsmittelmißbrauch wäre als „Rasterfahndung“ unzulässig.

Ein Gesundheitsamt wollte in seinem Bereich eine **umfassende Kontrolle** nach dem Betäubungsmittelgesetz durchführen. Hierzu sollten von allen betroffenen Ärzten die Betäubungsmittelrezepte angefordert sowie die Namen der Patienten, der Ärzte und die verordneten Medikamente erfaßt und überprüft werden. Auf diese Weise sollten z.B. Doppelverordnungen festgestellt werden. Das Gesundheitsamt hatte die Absicht, nach Abschluß der Aktion die Daten zu löschen. Eine dauerhafte Speicherung war nur für die Namen und Anschriften der Ärzte geplant.

Das Gesundheitsamt hatte Zweifel, ob ein solcher Abgleich zulässig sei und bat um eine datenschutzrechtliche Stellungnahme. Die Prüfung hat ergeben, daß das **Betäubungsmittelgesetz** das Gesundheitsamt nur **im Einzelfall** berechtigt, zu Kontrollzwecken Rezepte einzusehen. Die Ärzte sind nach der Betäubungsmittelverschreibungsverordnung verpflichtet, Durchschriften der Betäubungsmittelrezepte ganz oder teilweise drei Jahre aufzubewahren und auf Verlangen der zuständigen Landesbehörde einzusenden oder den Beauftragten die-

ser Behörde vorzulegen. Aus der Verordnung ergibt sich weiter, daß die Kreisgesundheitsbehörden im Rahmen ihrer Überwachungstätigkeit die bei den Ärzten befindlichen BTM-Rezepte kontrollieren dürfen. Diese Überwachungsrechte dürfen aber nicht dazu genutzt werden, aus den Unterlagen aller Ärzte eines Gesundheitsamtsbezirks nach Art einer „**Rasterfahndung**“ eine Gesamtdatenbank aller Patienten mit Betäubungsmittelanwendungen zu erstellen und sie in die Nähe von BTM-Abhängigen oder Drogensüchtigen zu rücken. Das wäre aber die Folge des beabsichtigten Verfahrens. Der Rahmen der Kontrolle des legalen Betäubungsmittelverkehrs würde damit überschritten und über die Kontrolle der Ärzte bzw. Apotheker hinaus eine allgemeine Patientenkontrolle eingeführt. Wir hielten diese Art der Auswertung für unverhältnismäßig und haben dringend davon abgeraten.

Zulässig wäre dagegen eine Auswertung, die zwar **patientenbezogen**, aber auf die jeweilige einzelne Arztpraxis beschränkt ist. Hierdurch kann das Verschreibungsverhalten des einzelnen Arztes und die Einhaltung der Mengengrenzung nach der Betäubungsmittelverschreibungsverordnung kontrolliert werden. Nach Abschluß der Kontrolle sind die Daten zu löschen.

4.6.2.2 Weitergabe amtsärztlicher Gutachten ohne Einwilligung des Betroffenen

Ist bei Beantragung einer Taxikonzession ein amtsärztliches Gutachten vorzulegen, so kann der Antragsteller bestimmen, ob es direkt dem Ordnungsamt zugeleitet oder zunächst ihm ausgehändigt wird. Wird dies nicht beachtet, liegt ein Verstoß gegen das informationelle Selbstbestimmungsrecht und gegen die ärztliche Schweigepflicht vor.

Das neue LDSG hat die Pflicht zur Löschung von Daten beträchtlich erweitert. So sind Daten, die unter Verstoß gegen Rechtsvorschriften verarbeitet wurden, grundsätzlich von Amts wegen zu löschen. Wie sich das auswirken kann, zeigt folgender Fall.

Ein Bürger hatte beim Ordnungsamt einen Antrag auf Ausstellung eines **Personenbeförderungsscheines** gestellt. Voraussetzung für die Erteilung ist unter anderem eine **amtsärztliche Untersuchung**. Er hatte sich mit der Untersuchung durch das zuständige Gesundheitsamt einverstanden erklärt. Das Ordnungsamt hat das zuständige Gesundheitsamt hiervon unterrichtet und zugleich schriftlich mitgeteilt: „Eine Erklärung zur Entbindung von der ärztlichen Schweigepflicht zur Mitteilung des Begutachtungsergebnisses an die Verwaltungsbehörde liegt hier nicht vor“. Die Untersuchung wurde durchgeführt. Obwohl der Betroffene nicht über das Ergebnis informiert und nicht um seine Einwilligung zur Weitergabe des Gutachtens gebeten wurde, schickte das Gesundheitsamt das Ergebnis des Gutachtens an das Ordnungsamt.

Wir haben diese Übermittlung als **unzulässige Offenbarung** von Daten, die dem Arztgeheimnis unterliegen, gewertet, die gegenüber dem zuständigen Gesundheitsamt förmlich zu beanstanden war.

Da die Datenübermittlung an das Ordnungsamt ohne Einwilligung des Betroffenen unzulässig war, war auch die **Speicherung** durch das Ordnungsamt **unzulässig**. Nach dem Landesdatenschutzgesetz waren diese personenbezogenen Daten daher zu löschen, was inzwischen auch geschehen ist.

4.6.2.3 Änderungen im Gesundheitsrecht

Das bereits verabschiedete Gesundheitsstrukturgesetz 1992 und das noch zu beratende Änderungsgesetz zum Sozialgesetzbuch enthalten auch Vorschriften zum Datenschutz. Nicht alle können im Interesse der Betroffenen als positiv angesehen werden.

Gesundheitsstrukturgesetz 1992

Das „Gesetz zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung“ ist am 01.01.1993 in Kraft getreten. Sein Ziel ist es, den Kostenanstieg in der gesetzlichen Krankenversicherung zu verringern. Da im Rahmen dieses Gesetzes auch eine Reihe datenschutzrelevanter Vorschriften geändert bzw. ergänzt werden, haben sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch der Landesbeauftragte hierzu Stellung genommen. Den **Bedenken** der Datenschutzbeauftragten ist in einer Reihe von Punkten **nicht Rechnung getragen** worden. Das Schwergewicht der politischen Diskussion lag vielmehr auf den Maßnahmen zur Eindämmung der Kosten. Wegen der zügigen parlamentarischen Beratung fehlte die Zeit für eine differenzierte Diskussion datenschutzrechtlicher Fragen.

Im einzelnen ging es um folgendes:

- Das Gesetz schreibt vor, daß die **Krankenkassen** in den Ländern **Modellvorhaben** zur Prüfung der Notwendigkeit von Krankenhausbehandlungen durchführen. Es fehlte zunächst eine Regelung bis wann die in diesem Zusammenhang bei den Medizinischen Diensten angefallenen personenbezogenen Daten zu löschen bzw. zu anonymisieren sind. Auf Anregung der Datenschutzbeauftragten hat der Gesetzgeber festgelegt, daß dies spätestens ein Jahr nach Abschluß des Modellvorhabens zu erfolgen hat.
- Das Gesetz läßt die weitgehende **maschinelle Erfassung** der **Leistungsdaten** der Versicherten zu. Damit könnte das Gesundheitsstrukturgesetz etwas zum Ergebnis haben, was nach einhelligem politischen Willen bislang bewußt vermieden wurde, nämlich ein **Leistungskonto** des Versicherten. Dies wäre wirklich ein entscheidender Schritt hin zum „**gläsernen Patienten**“. Es wird daher in Zukunft darauf an-

kommen, in der Praxis die Gefahr zu vermeiden, die mit der maschinellen Erfassung versichertenbezogener Daten und der Möglichkeit der schnellen Verknüpfung verbunden sind. Aus der beabsichtigten Kontrolle des ärztlichen Verordnungsverhaltens darf keine Kontrolle der Versicherten werden.

- Weiter ist der **Katalog der Daten** deutlich **erweitert** worden, die vom Krankenhaus an die Krankenkassen übermittelt werden dürfen. Neu ist, daß das Krankenhaus auch die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung hierfür zu übermitteln hat. Erstmals haben die Krankenhäuser auch Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen zu übermitteln. Insbesondere die Aufnahme der Operationen in diesen Übermittlungskatalog überzeugt nicht, da diese Daten in keinem Sachzusammenhang zu der Abrechnung stehen. Die Tatsache, daß die Möglichkeit für die Landesverbände der Krankenkassen und die Verbände der Ersatzkassen eröffnet wird, mit den Krankenhäusern bzw. Krankenhausgesellschaften Vereinbarungen zu treffen, wonach bei der Abrechnung von Leistungen auf einzelne Angaben verzichtet werden kann, zeigt, daß offensichtlich nicht alle der künftig zulässigen Datenübermittlungen erforderlich sind. Die derzeit anstehende Änderung des SGB bietet Gelegenheit, diesen Fehler zu korrigieren.
- Nach dem Entwurf der **Bundespfllegesatzverordnung** dürfen wahlärztliche Leistungen zwar durch privatrechtlich organisierte Abrechnungsstellen abgerechnet werden. Das Gesetz fordert nach Intervention der Datenschutzbeauftragten nunmehr aber die Einwilligung der Patienten, wenn Abrechnungsstellen eingeschaltet werden sollen.

Entwurf eines Änderungsgesetzes zum Sozialgesetzbuch

Zu diesem Gesetzentwurf haben wir wie folgt Stellung genommen:

- Der Entwurf sieht die Befugnis vor, Sozialdaten an **externe Gutachter** zu übermitteln. Für die Daten, die der Gutachter seinerseits erhebt, bedarf es einer Befugnis zur Übermittlung an den Auftraggeber. In der Praxis kann nämlich nicht immer die Einwilligung der betroffenen Versicherten eingeholt werden.
- Als problematisch ist zu werten, daß der Entwurf den bisher im SGB üblichen Begriff der **Offenbarung** durch den Begriff der **Übermittlung** ersetzen will. Dadurch wird der Schutz der Sozialdaten erheblich aufgeweicht. Nicht schon die Information einzelner unzuständiger Mitarbeiter derselben datenverarbeitenden Stelle wird untersagt, wie es bisher der Fall war. Die Sperre setzt vielmehr erst dann ein, wenn Informationen von einer datenverarbeitenden Stelle zu einer anderen fließen.

- Das SGB läßt schon heute **Datenoffenbarungen** und künftig auch **Datenübermittlungen** innerhalb des **gesamten Sozialleistungsbereichs** zu, soweit es für jegliche gesetzliche Aufgabenerfüllung nach dem SGB erforderlich ist. Damit ist für Sozialdaten keine auf den einzelnen Vorgang bezogene Zweckbindung gewährleistet. Sozialdaten genießen damit insoweit einen geringeren Schutz als sonstige Daten. Wir haben vorgeschlagen, das SGB X so zu ändern, daß die Nutzung und Übermittlung der Daten nur für die Erfüllung der jeweiligen einzelnen konkreten Aufgabe zulässig ist.
- Schließlich sieht der Entwurf die Möglichkeit des **Online-Zugriffs** auf Sozialdaten vor. Hiergegen bestehen große Bedenken, auch wenn der Zugriff nur innerhalb des Sozialleistungsbereichs vorgesehen ist. Für die jeweiligen Verfahren müssen vielmehr spezielle Regelungen durch Rechtsnormen geschaffen werden.

4.7 Kultusbereich

4.7.1 Studentendatenverordnung

Die Studentendatenverordnung muß nunmehr zügig verabschiedet werden. Die datenschutzrechtlichen Regelungen müssen wirksam in die Praxis der Studentenverwaltung und etwaige besondere Studien- und Prüfungsordnungen umgesetzt werden.

Bereits im Jahre 1990 verabschiedete der Schleswig-Holsteinische Landtag ein Änderungsgesetz zum Hochschulrecht, das einen Rahmen für die Verarbeitung personenbezogener Daten der Studienbewerber und der Studierenden schafft. Dabei werden die **Verwaltungszwecke**, zu deren Erfüllung die Daten verarbeitet werden sollen, auf „Hochschulzugang, Studium, Studienverlauf und Prüfung“ **begrenzt**. Die Detailregelung, welche einzelnen Daten für welche Zwecke verarbeitet oder sonst verwendet werden dürfen, aber einer besonderen Verordnung der Kultusministerin überlassen.

Diese **Verordnung** war im Berichtszeitraum Gegenstand der Erörterungen mit dem Ministerium. Die grundsätzliche Konzeption, die uns zur Stellungnahme zugeleitet wurde, erscheint geeignet, die Anlässe hinreichend klar zu bezeichnen, zu denen personenbezogene Daten verarbeitet werden müssen und die dafür erforderlichen Daten konkret zu benennen. Die Verordnung regelt verschiedene Phasen, z.B. „Zulassung“, „Einschreibung“, „Studienverlauf“, die Zweckbestimmungen für die Datenverarbeitung darstellen. Diesen Zwecken werden zu konkret aufgeführten Anlässen jeweils bestimmte Daten aus einem 32 Datenkategorien umfassenden Datenkatalog zugeordnet. Wir haben in unserer Stellungnahme auf Ungenauigkeiten in einzelnen Formulierungen hingewiesen, die in einer überarbeiteten Fassung bereinigt wurden.

Eine gewisse Unsicherheit erwächst aber daraus, daß neben diesen sehr konkreten Regelungen der Verordnung auch auf besondere „**Studien- und Prüfungsordnungen**“ hingewiesen wird, die sowohl die Verarbeitungszwecke als auch die dafür erforderlichen Daten näher und über den Katalog der Verordnung hinausgehend bestimmen können. Diese Vorschriften müssen dem geltenden Datenschutzrecht entsprechen oder unverzüglich angepaßt werden.

Weiter macht die Verordnung nicht hinreichend deutlich, welche Daten **freiwillig** vom Betroffenen preisgegeben werden. Es ist vorgesehen, die Unterschiede zwischen zwangsweise und auf freiwilliger Grundlage erhobenen Daten in der Gestaltung der entsprechenden Vordrucke und bei den Verfahrenserläuterungen klarzustellen. Dabei wird zu prüfen sein, ob eine solche Verfahrensweise ausreicht, um den Anforderungen des LDSG insbesondere an die Zweckbindung und die Verfahrenstransparenz zu entsprechen.

Mit diesen Einschränkungen kann davon ausgegangen werden, daß die Verordnung in brauchbarer Weise die Verarbeitung personenbezogener Studentendaten für die Studienverwaltung regelt. Der Entwurf sollte nunmehr zügig verabschiedet und in Kraft gesetzt werden.

4.7.2 Umfragen durch Elternvertretungen

Elternbeiräte dürfen im Rahmen ihrer Aufgaben die Meinung von Eltern zu Problemen der Schule und des Unterrichts erfragen. Sie bedürfen dazu keiner besonderen Genehmigung. Die Stellungnahmen der Eltern erfolgen freiwillig. Die Eltern sind darüber sowie über das weitere Verfahren und insbesondere über die beabsichtigte Weitergabe des Befragungsergebnisses zu unterrichten.

Der Landeselternbeirat für Grund-, Haupt- und Sonderschulen wollte die Eltern umfassend über die beabsichtigte Einführung von **Berichtszeugnissen** in der Grundschule befragen und die Ergebnisse in seiner Stellungnahme gegenüber der Kultusministerin verwerthen. In die **Befragung** wurden Elternvertretungen auf der Kreis- und Schulebene einbezogen. Wir sind mehrfach um Stellungnahme zur Rechtmäßigkeit gebeten worden.

Eine spezielle Rechtsvorschrift zu Meinungsumfragen durch Elternvertretungen besteht nicht. Wir sind ebenso wie die Ministerin der Auffassung, daß solche Umfragen durch Elternvertretungen zu schulbezogenen, die Eltern gemeinsam interessierenden Erziehungs- und Unterrichtsfragen **grundsätzlich zulässig** sind. Eine Genehmigung ist nicht erforderlich. Die Ermittlung und Vertretung der Elternmeinung gehört zu den Aufgaben von Elternvertretungen. Es bedarf dazu auch keiner Bestätigung durch den jeweiligen Schulelternbeirat, etwa durch einen förmlichen Beschluß. Es handelt sich dabei um zulässige Datenerhebungen, allerdings um solche auf freiwilliger Grundlage.

In der Praxis erhielten die Eltern einen vom Elternbeirat formulierten Brief, in dem sie über Ziel und Zweck der Befragung unterrichtet wurden. Der Brief enthielt weiter einen Zettel, auf dem die Eltern ankreuzen konnten, ob sie

- ein Notenzeugnis wie früher,
- ein Notenzeugnis mit Beurteilung oder
- ein Beurteilungszeugnis bis zum vierten Schuljahr ohne Ziffernnoten

bevorzugten. Als Ergebnis wurden teilweise die Coupons vollständig oder daraus zusammengefaßte Listen an die Kreiselternebeiräte und den Landeselternebeirat weitergegeben.

In den Elternbriefen war weitgehend korrekt von der Freiwilligkeit der Antwort die Rede. Es fehlte jedoch in der Regel der Hinweis, daß beabsichtigt sei, die Meinungsäußerungen weiterzugeben. Ein solcher Hinweis ist jedoch erforderlich, wenn der Schulelternebeirat die Voten der Eltern **personenbezogen** weitergeben möchte. Aus datenschutzrechtlicher Sicht war dies zu beanstanden.

4.7.3 Aufbewahrung von Klassenarbeiten

Klassenarbeiten werden in der Schule zwei Jahre aufgehoben und danach zurückgegeben, soweit die Schüler noch die gleiche Schule besuchen. Anderenfalls müssen sie vernichtet werden.

Ein Vater hat uns mitgeteilt, daß Klassenarbeiten seines Sohnes zwei Jahre lang verwahrt und dann von der Schule vernichtet würden, ohne Schüler und Eltern davon zu unterrichten. Gegen diese Verfahrensweise äußerte er Bedenken und bat um Überprüfung.

Die Aufbewahrung von Klassen- und Hausarbeiten ist durch Erlaß geregelt. Danach sollen **Klassenarbeitshefte** in der Regel **zwei Jahre** in der Schule aufbewahrt werden. Nach dieser Zeit sollen die Arbeiten an die Schülerinnen und Schüler **zurückgegeben** werden, wenn sie zu diesem Zeitpunkt noch der Schule angehören. Schülerarbeiten, die nicht zurückgegeben oder an ein Archiv abgegeben werden, sind zu vernichten.

Diese Regelung halten wir für sachgerecht. Wie der konkrete Fall gezeigt hat, kommen die Schulen der Rückgabeverpflichtung allerdings nicht immer unaufgefordert nach.

4.7.4 Bekanntgabe von Zensuren in der Klasse

Leistungsergebnisse von Schülern dürfen vor der Klasse erörtert werden, soweit das aus pädagogischen Gründen erforderlich ist. Nicht zulässig ist die Zusammenstellung und Bekanntgabe von „Ranglistenplätzen“ aufgrund der Ergebnisse von Intelligenztests.

Ein altes Problem taucht in unterschiedlicher Gestalt immer wieder auf: Nämlich die Frage, ob Leistungsbewertungen der

Schüler, z.B. die Ergebnisse der **Klassenarbeiten**, der **Klassenspiegel** oder auch die Ergebnisse von **Intelligenztests** in den Klassen bekanntgegeben werden dürfen. Obwohl von seiten der Eltern verschiedentlich Bedenken vorgetragen worden sind, haben wir bislang stets die Bekanntgabe von Zensuren und das Besprechen der Ergebnisse von Klassenarbeiten vor der versammelten Klasse datenschutzrechtlich als zulässig betrachtet. Die Schule hat nicht nur den Auftrag, Wissen zu vermitteln, sondern auch die Verpflichtung, pädagogisch auf die ihr anvertrauten Kinder einzuwirken und ihnen eine Einordnung der eigenen Leistung zu ermöglichen, um die nach dem Schulgesetz vorgegebenen Bildungs- und Erziehungsziele zu erreichen.

Etwas anders ist allerdings die rechtliche Situation zu beurteilen, wenn es sich um die Durchführung von **Intelligenztests** und um die **Bekanntgabe der Ergebnisse** an alle Eltern handelt. Kürzlich macht uns ein Vater auf einen solchen Intelligenztest aufmerksam, dessen Ergebnisse bei allen Schülern unzureichend anonymisiert und darüber hinaus an alle Eltern weitergegeben wurden. Er fand die Art und Form der Zusammenstellung der Intelligenzquotienten der Kinder mit den Zusatzangaben Geschlecht und Alter datenschutzrechtlich bedenklich. Dadurch war nach seiner Auffassung die Zuordnung der Kinder zu einem „Ranglistenplatz“ auch für Außenstehende möglich. Wir teilen diese Bedenken. Die Bekanntgabe solcher Informationen an die Eltern ist unzulässig, sofern nicht das Einverständnis der Betroffenen vorliegt. Dem schloß sich auch die Kultusministerin an.

4.7.5 **Klassenbücher einst und heute**

Der Inhalt von Klassenbüchern ist auf die Daten zu beschränken, die für die Durchführung des Unterrichts erforderlich sind. Sensible personenbezogene Schülerdaten wie Zensurenlisten und Aufzeichnungen von Ordnungsmaßnahmen sind getrennt zu führen und unter Verschuß zu halten.

Immer wieder werden Fragen nach Form und Inhalt der Klassenbücher sowie danach gestellt, was die Schulen bei der Aufbewahrung der **Klassenbücher** zu beachten haben.

Die älteren Klassenbücher enthielten eine umfangreiche Datensammlung über Schülerinnen, Schüler, Eltern und Lehrkräfte. Das neue **Schulgesetz** hat den zulässigen Datenumfang demgegenüber erheblich eingeschränkt. Die uns vorgelegten neuen Klassenbücher sollen nur noch solche personenbezogenen Eintragungen aufnehmen, die für die pädagogische Arbeit in der Schule und in der Klasse unerlässlich sind. Künftig enthält das Klassenbuch keine Adreßdaten und keine Telefonnummern mehr. Auch die Angaben „Geburtsort“ und „Krankenkasse“ entfallen. Das ist zu begrüßen. Wir haben ergänzend darauf hingewiesen, daß nach unserer Auffassung auch die Angabe der Religions- und Staatsangehörigkeit der Schülerinnen und Schüler entbehrlich ist.

Obwohl die Klassenbücher künftig weniger sensible Daten enthalten werden, haben die Schulen durch die Lehrkräfte sicherzustellen, daß die **Klassenbücher** außerhalb der Unterrichtszeit **verschlossen** aufbewahrt werden.

Getrennt von den Klassenbüchern geführt werden darüber hinaus sensiblere Individualdaten, z.B. in Form von Ergebnislisten über schriftliche Arbeiten und mündliche Leistungen (**Zensurenlisten**) sowie von Eintragungen über Erziehungskonflikte einschließlich etwaiger **Ordnungsmaßnahmen**. Diese Unterlagen sind in der Schule generell unter Verschuß zu halten.

4.8 Landwirtschaftsverwaltung

4.8.1 Neues Förderungssystem, perfekte Kontrolle

Demnächst sollen die Angaben von Landwirten in Förderanträgen per Satellit überprüft werden. Derzeit stehen lediglich noch die Kosten, nicht aber technische Gründe der Überwachung der Höfe aus dem Weltall entgegen.

In den vergangenen Jahren sind wir häufig von der Landwirtschaftsverwaltung um Beratung zu der Frage gebeten worden, welche Daten in welcher Weise im Rahmen der einzelnen **Subventions- und Förderungsverfahren** verarbeitet werden dürfen (vgl. z.B. Tz. 4.9.2 dieses Berichtes). Datenschutzrechtliche Probleme ergaben sich insbesondere deshalb, weil diese Leistungen i.d.R. nicht auf der Grundlage eines gesetzlichen Regelwerkes gewährt wurden (wie z.B. die Steuererstattungen oder die Sozialhilfe), sondern aufgrund **unterschiedlicher Richtlinien und Programme** und aus verschiedenen „Töpfen“ (Europäische Gemeinschaft, Bund, Land). Die bei der Festsetzung der Beträge zugrunde zu legenden Fördermerkmale waren meistens genauso vage beschrieben wie die Befugnis der gewährenden Behörden, die Angaben der Antragsteller plausibel zu überprüfen und ggf. mit Angaben in Anträgen auf anderweitige Fördermaßnahmen zu vergleichen.

Auch eine Verordnung des Bundeslandwirtschaftsministers aus dem Jahre 1989 brachte keine hinreichende Klarheit. Sie definierte zwar ein einheitliches Datenprofil. Dieses reichte aber nach Ansicht der Praktiker nicht aus, um alle in Frage kommenden Ausgleichszahlungen, Förderbeträge usw. richtig festsetzen zu können. Zwischen den für die Fördermaßnahmen zuständigen Behörden des Bundes und der Länder bestand zudem kein Einvernehmen darüber, wie und in welchem Umfang Antragsteller aufzuklären waren, z.B. über die Rechtsfolgen der Inanspruchnahme der Gelder, über die geplanten Datenübermittlungen zum Zweck des Abgleichs, über die statistischen Auswertungen, die Kontrollen und die Revisionsmaßnahmen. Die **Rechtslage** war so **verwirrend**, daß nicht einmal mit letzter Sicherheit festgestellt werden konnte, ob es zulässig

war, alle Anträge eines Landwirtes in einer Akte zusammenzufassen und unter einer „Stammnummer“ abzulegen.

Diese datenschutzrechtlich unbefriedigende Situation änderte sich, nachdem der **EG-Ministerrat** im Mai 1992 eine **Reform** der gemeinsamen Agrarpolitik beschlossen hatte. Das bisher geltende System der Einkommensstützung für bestimmte Erzeugnisse wurde abgelöst durch direkte flächen- bzw. tierbezogene Ausgleichszahlungen. Die verwaltungsmäßige Durchführung und Kontrolle dieser allein in Schleswig-Holstein jährlich mehr als 100 000 Verwaltungsakte ist durch bindende Vorgaben der EG ohne Ermessensspielräume für die jeweiligen Länder bzw. Behörden festgelegt. Das Verfahren wird als **„integriertes Verwaltungs- und Kontrollsystem“** zur Landwirtschaftsförderung (INVEKOS) bezeichnet und enthält folgende Elemente:

- Ermittlung der Ausgleichszahlungen auf der Basis der Größe einzelner „Schläge“ (Wiesen, Äcker) bzw. über Ohrmarken zu identifizierender Tiere (Kühe, Schafe);
- Erfassung von Flächen nicht nur hinsichtlich der Größe, sondern auch mit der geographischen Lage; zugelassen ist ein **automatisierter Abgleich** der Angaben der Landwirte mit **Satelliten- und Luftbildaufnahmen**, die über die aktuelle Größe und Nutzung landwirtschaftlicher Parzellen Auskunft geben;
- Aufbau kompatibler **Datenbanken mit Direktabrufmöglichkeit** zur Speicherung und Bereitstellung aller Informationen aus den Anträgen;
- feste Quoten für Antrags- und Vor-Ort-Kontrollen;
- Prämienrückforderung und Prämienausschluß von Landwirten, die unrichtige oder unvollständige Angaben gemacht haben;
- Überwachung der Kontrollmaßnahmen der Länder durch die EG, Rückforderungsansprüche gegenüber den Ländern, die nicht hinreichend kontrollieren.

Einerseits ist die Tatsache zu begrüßen, daß die Datenerhebungen zum Zweck der Festsetzung von Förderbeträgen für landwirtschaftliche Betriebe nunmehr auf eine klare Rechtsgrundlage gestellt werden. Andererseits ist zu bedauern, daß die Datenschutzbeauftragten des Bundes und der Länder nicht an der Gestaltung dieses Regelwerkes haben mitwirken können. Da es auf EG-Ebene (noch) keinen Datenschutzbeauftragten gibt, war es uns nicht möglich, dort beratend einzugreifen, wo die Landwirte im Ergebnis „gläsern“ gemacht werden.

Besonders ins Auge springt die vorgesehene Möglichkeit, landwirtschaftliche Betriebe mit Hilfe von **Satellitenaufklärung** zu beobachten. Wenn es einen Anlaß zu einer **intensiven Technikfolgenabschätzung** vor ihrem praktischen Einsatz gibt, dann dürfte er in diesem Fall gegeben sein. Einer der Gründe für die Schaffung der Datenschutzgesetze war die in den Innenverwaltungen bestehende Absicht, das staatliche

Meldewesen durch die Personenkennzeichen zu rationalisieren. Satelliten- und „Luftaufklärung“ sind mindestens ebenso gravierende Einschnitte in die Persönlichkeitsrechte der Betroffenen. Ein nicht hinreichend reflektierter Einsatz dieser technischen Möglichkeiten beschwört die Gefahr herauf, daß Entwicklungen in Gang gesetzt werden, deren **Spätfolgen** niemand in Kauf nehmen will.

In Schleswig-Holstein werden zirka 25 000 Landwirte antragsberechtigt sein. Die Zahl wird sich in den nächsten Jahren eher verringern als ansteigen. Für die Bearbeitung dieser „Fälle“ sind sechs Ämter für Land- und Wasserwirtschaft zuständig. Darf man den dort tätigen orts- und sachkundigen Beamten wirklich nicht zutrauen, daß sie aus den jeweils zirka 4 000 „Kunden“ die wenigen „schwarzen Schafe“ auch ohne Satellitenhilfe herauspicken?

Wir hoffen, daß wir vom Minister für Ernährung, Landwirtschaft, Forsten und Fischerei vor der Realisierung derart einschneidender technischer Verfahrensweisen Gelegenheit zu einer **gutachterlichen Stellungnahme** erhalten. Das gilt auch bezüglich der Aufklärung der Landwirte über die Rechtsfolgen ihrer Antragstellung. Diese ist zwar grundsätzlich freiwillig. Da es sich aber um einen existenznotwendigen Einkommensausgleich handelt, kann sich faktisch kein Landwirt dem Verfahren entziehen. Die öffentliche Ankündigung des Landwirtschaftsministers, daß er in den Ämtern für Land- und Wasserwirtschaft nicht genügend Personal zur persönlichen Beratung bereitstellen könne, bedingt eine ganz besonders wirksame (faire) schriftliche Aufklärung. Das Landesdatenschutzgesetz schreibt nämlich zwingend vor, daß die Antragsteller **in geeigneter Weise** über die Bedeutung der Einwilligung (in diesem Fall der Antragstellung), insbesondere über den Verwendungszweck der Daten und bei beabsichtigten Datenübermittlungen auch über den Empfängerkreis aufzuklären sind.

4.8.2 Fehler, die sich nicht bezahlt machen

Die tatsächlichen Gründe für Datenerhebungen sind den Betroffenen bekanntzugeben. Fehlerhafte Datenerhebungen führen zu rechtswidrigen Datenspeicherungen.

Seit einigen Jahren **fördert** der Minister für Natur, Umwelt und Landesentwicklung Landwirte, die bereit sind, Teile ihrer landwirtschaftlich genutzten **Flächen stillzulegen** (zu extensivieren) und so zur Schaffung von Biotopen beizutragen. Das Verfahren, durch das die zur Verfügung stehenden Förderungsbeträge verteilt werden, ist vergleichsweise kompliziert. Zunächst ist ein Antrag zu stellen. Wird über diesen unter Berücksichtigung der Förderungswürdigkeit und der vorhandenen Geldmittel positiv entschieden, kommt es zum Abschluß eines Vertrages, in dem die Verpflichtungen des Landwirtes und seine Ansprüche auf Entschädigungszahlungen detailliert festgelegt sind. Es handelt sich also nicht um ein „normales“ Verwaltungsverfahren, das mit einem rechtsmit-

telfähigen Bescheid endet (vgl. Tz. 4.9.1 dieses Berichtes), sondern gleichsam um „fiskalisches“ Handeln des Staates, das durch Unterschrift unter eine Vereinbarung rechtswirksam wird. Der privatrechtliche Charakter dieses Rechtsgeschäfts wird noch dadurch betont, daß die Antragsbearbeitung und die Vertragsabwicklung der Schleswig-Holsteinischen Landgesellschaft mbH übertragen worden sind.

Diese Konstruktion erlangte in einem Konfliktfall, auf den uns der Bauernverband Schleswig-Holstein aufmerksam machte, wesentliche datenschutzrechtliche Bedeutung. Nachdem die ersten zeitlich befristeten Verträge mit den Landwirten ausgelaufen waren, wurden sie befragt, ob sie weiterhin an diesem (inzwischen modifizierten) Programm teilnehmen wollten. Die ihnen übersandten Vordrucke sollten aber auch dann „unbedingt“ (zumindest teilweise) ausgefüllt „umgehend“ zurückgesandt werden, wenn kein Interesse an einem erneuten Vertragsabschluß bestand. Hinter dieser Aufforderung versteckte sich der Versuch der **nachträglichen Fehlerkorrektur**. Um die Kosten für dieses Förderprogramm von der EG erstattet zu bekommen, mußte das Land bestimmte Verwendungsnachweise erbringen. Die hierfür erforderlichen Daten waren aber in den „Altverträgen“ gar nicht enthalten. So entschloß man sich zu dem Versuch einer Nacherhebung nach Ablauf der Verträge, ohne die Landwirte darüber aufzuklären, worum es ging.

Zu Recht sah der Bauernverband darin eine **datenschutzrechtlich unzulässige Maßnahme**. Deshalb erging an den Minister für Natur, Umwelt und Landesentwicklung als Fachaufsichtsbehörde die Aufforderung, entweder die Aufklärung und die Einwilligung nachholen zu lassen, oder aber die bereits gespeicherten Daten (viele Landwirte hatten nämlich die Angaben in der Annahme, sie seien dazu verpflichtet, nachgeliefert) löschen zu lassen, da die Datenerhebung in dieser Form unzulässig war. Dieser Forderung hat der Minister nunmehr entsprochen.

In diesem Fall gab nicht nur der Versuch der „Nachbesserung“ zu datenschutzrechtlichen Bedenken Anlaß. Auch die Übertragung von Verwaltungsaufgaben auf ein privatwirtschaftliches Unternehmen sorgte für Verwirrung. Das „beliehene Unternehmen“ war sich offenbar der Tatsache, daß es insoweit als „nachgeordnete Verwaltung“ unter der Regie des weisungsbefugten Ministeriums tätig wurde, gar nicht bewußt. Anders ist nicht zu erklären, daß z.B. für die Weitergabe der Daten an die Fachaufsichtsbehörde – die Voraussetzung dafür war, den Antrag überhaupt zu bearbeiten – die Einwilligung der Landwirte eingeholt wurde. Auf der anderen Seite fehlte jeder Hinweis auf die Rechtsgrundlagen der Aktivitäten der Landgesellschaft.

Mehrere Jahre nach Beginn dieser Fördermaßnahmen wurden die Erhebungsvordrucke und die Vertragsmuster aufgrund unserer Beanstandungen nunmehr den datenschutzrechtlichen Gegebenheiten angepaßt. Im Interesse der Landwirte wäre zu wünschen, daß dies bereits zu Beginn der Fördermaßnahmen geschehen wäre.

5. Datenschutz bei den Gerichten

5.1 Datenschutzrechtliche Beratung von Gerichten

Das Landesdatenschutzgesetz gilt grundsätzlich auch für die Gerichte. Von Bedeutung sind insbesondere die Vorschriften über die Datensicherheit. Aber auch bei der Anwendung des Prozeßrechts muß der Datenschutz berücksichtigt werden.

Gerichte unterliegen zwar nicht der Kontrolle durch den Landesbeauftragten für den Datenschutz, soweit sie in richterlicher Unabhängigkeit tätig werden. Sie können sich aber von ihm datenschutzrechtlich beraten lassen. Davon haben Gerichte auch im vergangenen Jahr Gebrauch gemacht. Dabei haben wir unter anderem auf folgendes hingewiesen:

Auch Richter müssen **Datenschutz** beachten, selbst wenn sie in **richterlicher Unabhängigkeit** tätig werden. Dies ergibt sich aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 und Abs. 3 und aus dem LDSG. Die Bestimmungen des LDSG gelten auch für die Gerichte, soweit nicht besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln. Zwar enthalten die Prozeßordnungen eine Fülle von Vorschriften zur Datenverarbeitung, die dem LDSG vorgehen. Es bleiben aber Lücken, die aus dem LDSG zu schließen sind.

Dies gilt in besonderem Maße für die Regelungen zu den technisch-organisatorischen Maßnahmen zur **Datensicherheit** nach § 7 LDSG, die in den Prozeßvorschriften keine Entsprechung haben. Dabei ergibt sich vor allem im Hinblick auf den **Publikumsverkehr in Gerichtsgebäuden** die Notwendigkeit, Akten und sonstige Unterlagen mit personenbezogenen Daten vor unbefugter Kenntnisnahme zu schützen. Der Einwand, es herrsche ohnehin das Prinzip der öffentlichen mündlichen Verhandlung, verfängt nicht. Denn die Öffentlichkeit der Gerichtsverhandlung dient nicht dem Zweck, personenbezogene Daten über die Verfahrensbeteiligten zu erfahren, sondern der Kontrolle der Gerichte durch die Öffentlichkeit. Außerdem ist der Akteninhalt nicht identisch mit den in der mündlichen Verhandlung vorgetragenen Informationen. Hinzu kommt, daß die Flüchtigkeit des in mündlicher Verhandlung gesprochenen Wortes weniger Gefährdungen für das Persönlichkeitsrecht der Betroffenen mit sich bringt als die Einsichtnahme in Akten und sonstige Unterlagen. Es muß überdies bedacht werden, daß die Öffentlichkeit unter bestimmten Voraussetzungen von der Teilnahme an der Verhandlung ausgeschlossen werden kann.

Weiterhin haben wir auf schon früher behandelte datenschutzrechtliche Fragestellungen im Zusammenhang mit der Prozeßführung hingewiesen. So ist zum Beispiel bei der **Beauftragung von Gutachtern** sowohl im Rahmen der Versendung der für den Gutachter notwendigen Prozeßakten als auch bei der Adressierung dieser Unterlagen das Persönlichkeitsrecht der Betroffenen zu beachten (vgl. 12. TB, S. 53). Die Begründung

für Anträge auf **Prozeßkostenhilfe** darf auch nach der Rechtsprechung des Bundesgerichtshofs der Gegenseite nicht zur Kenntnis gebracht werden (vgl. 14. TB, S. 56).

5.2 Anspruch auf rechtliches Gehör contra Datenschutz

Gutachten über die Prozeßfähigkeit von Parteien können sensible personenbezogene Daten enthalten. Im Rahmen des rechtlichen Gehörs kann die Gegenseite Einblick verlangen. Datenschutz und rechtliches Gehör müssen in solchen Fällen in Konkordanz gebracht werden.

In einer Eingabe beschwerte sich ein Bürger über die Handhabung eines ihn betreffenden **Gutachtens** im Rahmen eines Zivilprozeßstreits. Er war auf seine **Prozeßfähigkeit** untersucht worden und hatte den Gutachter gebeten, den Prozeßgegnern nur das Ergebnis der Begutachtung mitzuteilen, nicht aber den detaillierten Befundbericht. Daraufhin erstellte der Gutachter „Teil 1“ des Gutachtens, in dem sich allgemeine Ausführungen zur Prozeßfähigkeit sowie das Ergebnis der Untersuchung befanden. In einem weiteren „Teil 2“ waren intime Daten über die Lebensgeschichte des Petenten, seine Krankheiten, sein Familienleben etc. enthalten. Später wurden seitens des zuständigen Richters beide Teile des Gutachtens auch der Gegenpartei bekanntgegeben.

Wir mußten dem Petenten mitteilen, daß wir für die Kontrolle der Gerichte nicht zuständig sind und deshalb in seiner Angelegenheit nicht tätig werden konnten. Wir hatten uns aber bereits unabhängig von dieser Petition anlässlich eines konkreten Falles, über den der Bayerische Landesbeauftragte für den Datenschutz berichtet hatte, an den Justizminister gewandt und dabei die Auffassung vertreten, auch bei der Bekanntgabe von Gutachten an die Gegenpartei im Rahmen von Zivilprozessen müsse das Recht auf informationelle Selbstbestimmung beachtet werden. Allerdings ist dabei in Rechnung zu stellen, daß der Anspruch auf rechtliches Gehör Verfassungsrang besitzt und nicht von vornherein davon ausgegangen werden kann, daß das Recht auf informationelle Selbstbestimmung überwiegt.

Zu bedenken ist aber auch, daß ohnehin nicht durchgängig gewährleistet ist, daß im Rahmen des Anspruchs auf rechtliches Gehör der Gegenseite sämtliche für das Verfahren relevanten Akten vorliegen. Nach der **Verwaltungsgerichtsordnung** kann beispielsweise die Vorlage von Akten verweigert werden, wenn das Bekanntwerden ihres Inhalts dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten würde. Wir haben deshalb angeregt zu prüfen, ob in vergleichbaren Fällen nicht „Teil 2“ von Gutachten außerhalb der eigentlichen Verfahrensakten aufbewahrt werden und damit der Einsichtnahme durch die Gegenpartei entzogen werden könnte.

Dieser Auffassung ist der **Justizminister** nicht gefolgt. Er hält die Aufteilung von Gutachten und die unterschiedliche Aufbe-

wahrung von Gutachtenteilen für nicht zulässig. Nach seiner Auffassung genießt der **Anspruch auf rechtliches Gehör** insoweit **Vorrang**. Der Justizminister sieht allenfalls im Rahmen der sorgfältigen und präzisen Formulierung von Gutachtenaufträgen sowie in Form eines Hinweises an die zu untersuchende Partei, daß die Ergebnisse der Untersuchung auch der Gegenpartei bekanntgemacht werden müssen, Möglichkeiten, das Recht auf informationelle Selbstbestimmung der Betroffenen zu verbessern.

6. Ordnungsmäßigkeit der Datenverarbeitung

6.1 Prüfungen im Bereich der automatisierten Datenverarbeitung

6.1.1 Erst ins Wasser springen, dann das Schwimmen lernen?

Der Einsatz informationstechnischer Systeme in Behörden setzt aus Sicherheitsgründen eine eingehende Planung sowie aufbau- und ablauforganisatorische Änderungen voraus, bevor mit dem praktischen Betrieb begonnen wird. Dies war bei einem geprüften Amt für Land- und Wasserwirtschaft nicht beachtet worden.

Viele Behörden im Landesbereich, aber auch die meisten Kommunen, werden in der Weise an die automatisierte Datenverarbeitung herangeführt, daß sie zunächst an **zentralen Verfahren**, die in der Regel von der Datenzentrale oder anderen Softwarehäusern und Rechenzentren betrieben werden, teilhaben. In diesen Fällen finden wesentliche Teile der Datenverarbeitung außer Haus statt. Die zu verarbeitenden Daten werden vor Ort erfaßt, dem Rechenzentrum zugeleitet und dort verarbeitet. Die maschinell erzeugten Bescheide und sonstigen Unterlagen gelangen in Papierform zurück und werden nach einer Schlußprüfung versandt. Die Akten enthalten weiterhin alle relevanten Verwaltungsdaten auf papierenden Datenträgern. Die EDV-Dateien im Rechenzentrum dienen nur als „Arbeitskopien“. Die zugrundeliegende Software wird in der Regel zentral getestet und zum Einsatz freigegeben. In den Behörden sind folglich nur geringe aufbau- und ablauforganisatorische Veränderungen erforderlich. Typische „Vertreter“ dieser Datenverarbeitungskonzeption sind die Basisversionen des Einwohnerinformationssystems, des Besoldungs- und Vergütungs-, des Wohngeld- sowie des BAföG-Verfahrens der Datenzentrale.

Nimmt dann die Zahl der auf diese Weise betriebenen automatisierten Verfahren zu und will man Anwendungen der Textbearbeitung und Bürokommunikation einbeziehen, stehen die Behörden irgendwann vor dem Problem, im eigenen Hause ein Rechnersystem zu installieren und sich **datenverarbeitungstechnisch selbständig** zu machen. Die sich daraus ergebenden personellen, technischen und organisatorischen Kon-

sequenzen werden allerdings häufig unterschätzt. Dies zeigte sich auch im Rahmen einer Prüfung bei einem **Amt für Land- und Wasserwirtschaft**, dem nach dem Willen des Ministers für Ernährung, Landwirtschaft, Forsten und Fischerei bei der Einführung der dezentralisierten Informationstechnik eine Art Pilotfunktion zukommen sollte.

Die dort bei einer **Kontrolle** vorgefundenen Schwachstellen lassen sich wie folgt zusammenfassen:

- Die Installation des Rechnersystems, an das bereits in der ersten Ausbaustufe 16 Terminals angeschlossen waren, ist zwar vom Ministerium für Ernährung, Landwirtschaft, Forsten und Fischerei angewiesen worden, eine Beschreibung und verbindliche Festlegung der damit verbundenen **aufbau- und ablauforganisatorischen Änderungen** wurde der Behörde jedoch nicht „mitgeliefert“.
- Ein einige Jahre zuvor entwickeltes **Gesamtkonzept** für die Automation in den Ämtern für Land- und Wasserwirtschaft wurde nicht fortgeschrieben und war also **veraltet**. Somit bestanden keine Hilfestellungen bei der Entscheidung der Frage, in welchen Ausbaustufen die Verfahren und das informationstechnische System weiterentwickelt werden sollten und welche Konsequenzen bereits zu Beginn des Betriebes aus der geplanten künftigen Entwicklung zu ziehen waren.
- Es war seitens des Ministeriums für Ernährung, Landwirtschaft, Forsten und Fischerei geplant, das System in einem weitgehend operatorlosen Betrieb zu fahren und die „kritischen“ Systemfunktionen im Rahmen einer **Fernwartung** zentral zu steuern. Die dafür erforderliche systemnahe Software war im Zeitpunkt der Installation des Betriebssystems aber noch gar nicht fertig. Somit war auch unklar, welche Funktionen die sogenannten Systemkoordinatoren auszuüben hatten, welche Qualifikationen für ihre Arbeit erforderlich und welche Überwachungsfunktionen den büroleitenden Beamten zuzuweisen waren.
- Eine **Dienstanweisung** für das im Zeitpunkt der Prüfung installierte informationstechnische System und die weiteren Personalcomputer **bestand nicht**. Dementsprechend gab es auch keine Festlegungen über den **Test und die Freigabe** von Software. Das galt auch für Programme und Prozeduren, die Mitarbeiter des Amtes für Land- und Wasserwirtschaft selbst entwickelt haben.
- Die Systemaktivitäten wurden **nicht revisionsfähig dokumentiert**.
- Der zuständige **Dezernent** war **nicht so ausgebildet** worden, daß es ihm möglich war, die Tätigkeit seiner Mitarbeiter im Bereich der Systembetreuung wirksam zu **überwachen**.

Die informationstechnische Situation in dieser Behörde ließ sich also recht gut in der Weise beschreiben, daß man erst

einmal begonnen hatte, Daten automatisiert zu verarbeiten, bevor die dafür unabdingbaren Regelungen ergangen waren.

Wir haben diese Vorgehensweise wegen des Verstoßes gegen die im Landesdatenschutzgesetz festgelegten Datensicherungs- und Überwachungsgebote **beanstandet** und sowohl den Minister für Ernährung, Landwirtschaft, Forsten und Fischerei als weisungsbefugte Aufsichtsbehörde als auch das Amt für Land- und Wasserwirtschaft zur **Mängelbeseitigung** aufgefordert. Die diesbezüglichen Aktivitäten liefen zunächst zögerlich an. Man rüstete zwar auch die anderen Ämter für Land- und Wasserwirtschaft mit Informationstechnik aus. In Anbetracht der Tatsache, daß auf allen Systemen zunächst im wesentlichen nur Textbearbeitung und Datenerfassung betrieben wurden, meinte man jedoch nach wie vor, die grundsätzlichen organisatorischen und technischen Regelungen erst zu einem späteren Zeitpunkt treffen zu können. Bezeichnend war die Kennzeichnung einer auf unser Drängen geschaffenen Dienstanweisung als „vorläufig“. Ungeklärt blieb beispielsweise die Frage, ob das in ihr geregelte Verfahren vorläufig war oder ob das Verfahren zwar endgültig, die Verfahrensregelungen aber noch nicht abschließend definiert waren.

Die Situation änderte sich schlagartig, als die unter Tz. 4.9.1 dieses Berichtes beschriebene **Reform der EG-Agrarpolitik** in den Ämtern für Land- und Wasserwirtschaft zu bewältigen war. „Aus dem Stand“ mußten nun viele neue automatisierte Verfahren realisiert und eingesetzt werden, die praktisch alle unsere Forderungen an die Sicherheit und Ordnungsmäßigkeit zwingend voraussetzten.

- In allen Ämtern für Land- und Wasserwirtschaft mußten als neue Organisationseinheiten sogenannte **IT-Leitstellen** eingerichtet werden.
- Da die Rechnerkapazitäten zu verdoppeln waren, mußte die **Systembetreuung** straff organisiert werden (Ausbildung, Vertretungsregelung, Zuständigkeiten, Definition der Schnittstellen zur Datenzentrale und zum Automationsreferat des Ministeriums für Ernährung, Landwirtschaft, Forsten und Fischerei).
- Die zuständigen Dezernenten mußten kurzfristig in ihre neuen Aufgaben **eingewiesen** werden.
- Die Datensicherungsmaßnahmen waren darauf abzustellen, daß mit Hilfe der automatisierten Verfahren Millionenbeträge ausgezahlt werden und riesige **revisionsfähige Datenbestände** über lange Zeiträume vorzuhalten sind.
- Im Hinblick auf die Softwarepflege bedurfte es neuer und vor allen Dingen einheitlicher **Dokumentationsmethoden** für Programme und Verfahren.
- Die Lösung **weiterer Problemstellungen** wie die Abnahme, Freigabe, Verteilung und Versionsverwaltung von Programmen, der Schutz gegen Datenverluste, der Transport, die Archivierung, die Löschung und die Entsorgung von

Datenträgern, der Brandschutz, die unterbrechungsfreie Stromversorgung usw. erlangte plötzlich höchste Priorität.

Der Minister für Ernährung, Landwirtschaft, Forsten und Fischerei hat uns über seine Aktivitäten laufend informiert und sich beraten lassen. Wenn in den vorgelegten Verfahrensregelungen auch noch recht häufig „in Vorbereitung“ zu lesen ist, so ist doch erkennbar, daß die im Rahmen der Prüfung erhobenen datenschutzrechtlichen Forderungen nunmehr umgesetzt werden. Diese zeitlichen und personellen Engpässe wären zu vermeiden gewesen, wenn bereits in der Pilotphase auf der Basis eines sorgfältig ausgearbeiteten **Organisations- und Sicherheitskonzeptes** gearbeitet worden wäre. Dieses Problem begegnet uns in zunehmendem Maße in allen Verwaltungsbereichen und verlangt eine allgemeinverbindliche administrative Lösung. Die zu erlassende Verordnung nach § 7 Abs. 4 LDSG dürfte hierzu Gelegenheit bieten (vgl. Tz. 6.3.1 dieses Berichtes).

6.1.2 Die automatisierte Datenverarbeitung einer Großstadt

Die Organisation der automatisierten Datenverarbeitung muß ständig den tatsächlichen technischen Gegebenheiten angepaßt werden. Ein veraltetes Regelwerk ist in der Praxis ein ebenso großes Sicherheitsrisiko wie fehlende Regelungen. Eine Kontrolle bei der Landeshauptstadt Kiel führte zu Beanstandungen.

Nach der Hansestadt Lübeck, der Datenzentrale, den Rechenzentren der Oberfinanzdirektion und der Ortskrankenkassen sowie der Landesversicherungsanstalt haben wir mit der **Landeshauptstadt Kiel** im abgelaufenen Jahr einen weiteren der ganz „großen“ öffentlichen Datenverarbeiter in unserem Zuständigkeitsbereich einer Prüfung hinsichtlich der Sicherheit und Ordnungsmäßigkeit der automatisierten Verfahren unterzogen. Dabei zeigte sich einmal mehr, daß die datenschutzrechtlichen Problemstellungen bei den vorgenannten datenverarbeitenden Stellen trotz unterschiedlicher Aufgabenstellungen und historischer Entwicklungen (diesen Begriff kann man im Bereich der EDV für einen Zeitraum von nur 25 Jahren durchaus benutzen) in ihren Grundstrukturen zwar nahezu identisch sind, daß aber die Lösungen sehr „individuell“ auf die jeweiligen rechtlichen, personellen und örtlichen Gegebenheiten abgestimmt sein müssen, um die nötige Effektivität zu erzielen.

Die automatisierte Datenverarbeitung der **Landeshauptstadt Kiel** ist gekennzeichnet durch eine außergewöhnliche **Heterogenität** und ein signifikantes **Volumen**. Obwohl im Rahmen der Prüfung wegen der fehlenden zentralen Dokumentation (s.a. weiter unten) die genauen Zahlen nicht ermittelt werden konnten, läßt sich feststellen, daß für die Verwaltung dieser rund 250 000 Einwohner zählenden Stadt

- mehr als 54 Rechnersysteme unter der Steuerung von
- 9 unterschiedlichen Betriebssystemen mit einer Kapazität von
- mehr als 350 MB Hauptspeicher und
- mehr als 1 900 MB Festplattenspeicherplatz sowie
- mehr als 400 Bildschirmterminals und
- mehr als 120 Druckerterminals eingesetzt werden.

Welches Volumen an Software mit Hilfe dieser Hardware zum Einsatz gelangt, läßt sich an zwei Zahlen deutlich machen: Allein für die vielfältigen Auswertungen aus dem Melderegister sind mehr als 500 Haupt- und Unterprogramme erforderlich. Das Gesamtverfahren „Personalwesen“ setzt sich aus ca. 850 Haupt- und Unterprogrammen zusammen, durch die über 200 Dateien in ca. 50 Abläufen verwaltet werden.

Eine vollständige Bestandsaufnahme und datenschutzrechtliche Überprüfung der gesamten Software und der damit verbundenen automatisierten Verwaltungsabläufe hätte unter diesen Gegebenheiten den zeitlich vorgegebenen Rahmen der Prüfung gesprengt. Aber bereits eine **stichprobenweise** Überprüfung führte zu zahlreichen **Beanstandungen**, deren Zielrichtung sich an einer Auswahl der wichtigsten Vorschläge aufzeichnen läßt, die wir zur Verbesserung des Datenschutzes gemacht haben:

– **Klarstellung der Aufbauorganisation**

Es sollte dem EDV-Leiter nicht formell die „fachliche und personelle Verantwortung für das gesamte Informationsgeschehen“ übertragen sein, wenn die Datenverarbeitung in den Fachämtern tatsächlich längst ein Eigenleben führt.

– **Überarbeitung und Ergänzung der ablauforganisatorischen Regelungen**

Dienst- und Geschäftsanweisungen sollten aktuell sein und so formuliert werden, daß sie klare Handlungsanweisungen für die jeweiligen Adressaten darstellen. Ein Abweichen von den Anweisungen sollte nur mit ausdrücklicher schriftlicher Genehmigung des jeweiligen Amtsleiters möglich sein.

– **Übernahme der Verantwortung durch die anweisende Ebene**

Die Einbeziehung von „Spezialisten“ auf der sachbearbeitenden Ebene (Programmierer, Systemkoordinatoren usw.) darf nicht dazu führen, daß kontrollfreie Räume entstehen. Die anweisende Ebene muß in die Pflicht genommen werden, die automatisierten Verfahren in ihrem Zuständigkeitsbereich zumindest in dem gleichen Maße zu beherrschen, wie es bei der konventionellen Abwicklung des Verwaltungshandelns als selbstverständlich angesehen wurde.

– **Definition der Aufgaben der EDV-Koordinatoren**

Mit der Aufgabe der EDV-Koordination sollten nur Mitarbeiter betraut werden, die über die erforderliche Fachkunde

auf dem Gebiet der Datenverarbeitung (ausgerichtet auf die tatsächlichen Konfigurationen und Anwendungen in dem jeweiligen Bereich), des Datenverarbeitungs- und des Datenschutzes sowie der Verfahrensinhalte verfügen.

– **Neuregelung der Auftragsdatenverarbeitung**

Es sollte in den vertraglichen Vereinbarungen mit dem Rechenzentrum exakt beschrieben werden, durch welche Maßnahmen gewährleistet wird, daß dieses keinen Zugriff auf die Daten bzw. keine sonstigen Einflußmöglichkeiten auf die Produktionsabläufe der Stadt Kiel hat.

– **Schaffung von Sicherheitskonzepten für die Hardware-Komponenten**

Für alle Hardware-Komponenten, die über ein veränderbares Betriebssystem, Programmspeicher usw. verfügen (insbesondere also auch für PC), sollten schriftliche Sicherheitskonzepte erstellt werden, aus denen hervorgeht, welche konkreten Risiken durch welche Maßnahmen auf ein vertretbares Maß reduziert worden sind.

– **Verbesserung des Test- und Freigabeverfahrens**

Das Test- und Freigabeverfahren sollte nicht für die einzelnen Anwendungen unterschiedlich, sondern allgemeinverbindlich festgeschrieben werden. Dabei sollten die testenden Stellen verpflichtet werden, Art und Umfang der Tests so zu dokumentieren, daß später deren Intensität und Ergebnisse nachvollzogen werden können.

– **Realisierung einer umfassenden und einheitlichen Hard- und Software-Dokumentation**

In Anbetracht des umfangreichen Hard- und Software-Potentials und um der Verpflichtung aus dem Landesdatenschutzgesetz, ein „Geräteverzeichnis“ über die eingesetzten Geräte, Betriebssysteme und Programme zu führen, nachzukommen, sollte an einer zentralen Stelle eine Hard- und Softwareregistrierung erfolgen. Es muß im Ergebnis möglich sein, zu jedem Zeitpunkt festzustellen, wo welche Hardware und welche Software zu welchen Zwecken installiert ist. Für die Dokumentation von Software sollten einheitliche und umsetzbare Mindestanforderungen für alle Organisationseinheiten, denen die Befugnis erteilt worden ist, Software zu erstellen und/oder zu implementieren, festgelegt werden. Die Erstellung und Fortschreibung dieser Dokumentation sollte zwingende Voraussetzung für die Freigabe der Verfahren zum Einsatz sein.

– **Beschreibung der Funktion der EDV-Abteilung als „Software-Haus“ und „Rechenzentrum“**

In Anbetracht der Tatsache, daß die Software-Erstellung durch eine besondere Abteilung für Informationstechnik lediglich eine Dienstleistung darstellt, sollte die Verantwortung der jeweiligen Fachämter für die Rechtmäßigkeit und

Richtigkeit der betreffenden Verwaltungsverfahren eindeutig klargelegt werden. Dem „Software-Haus“ müßte darüber hinaus vorgegeben sein, in welcher Form und mit Hilfe welcher Methoden die automatisierten Verfahren zu entwickeln und zu dokumentieren sind. Diese Verfahrensregeln sollten für alle Projekte einheitlich und verbindlich sein. Aus Verantwortungs- und Sicherheitsgründen sollte zwischen der „Verfahrensentwicklung“ und dem „Rechenzentrum“ unterschieden werden.

– **Verbesserung der Datensicherungsmaßnahmen in den Fachämtern**

Die Fachämter sollten jeweils für ihren Verantwortungsbereich ein schriftliches Sicherheitskonzept erstellen, das dem Datenschutzbeauftragten und der Abteilung für Informationstechnik zur Stellungnahme vorgelegt wird. Soweit an sich erforderliche Maßnahmen aus personellen, räumlichen oder finanziellen Gründen nicht ergriffen werden können bzw. sollen, müßte diese Entscheidung dem zuständigen Dezernenten vorbehalten werden. Um ein einheitliches Sicherheitsniveau zu erreichen, sollten in einer Dienstanweisung Mindestanforderungen an die Maßnahmen zur Datensicherheit definiert werden.

– **Optimierung der Schulungsmaßnahmen**

Die datenschutzrechtliche Belehrung aller Mitarbeiter, die dienstlich mit personenbezogenen Daten in „Kontakt“ kommen, und die spezielle (arbeitsplatzbezogene) Schulung derjenigen Personen, die mit der Entwicklung, der Steuerung oder der Benutzung automatisierter Verfahren befaßt sind, sollte verbindlich vorgeschrieben werden. Soweit Aufgabenstellungen spezielle Kenntnisse oder Fähigkeiten voraussetzen, sollten die betreffenden Mitarbeiter mit ihnen erst betraut werden, nachdem sie entsprechend geschult worden sind.

– **Bessere personelle Ausstattung des Datenschutzbeauftragten**

Dem Sozialdatenschutzbeauftragten sind die Personal- und Sachmittel zur Verfügung zu stellen, die es ihm ermöglichen, seinen gesetzlichen Verpflichtungen aus dem Sozialgesetzbuch nachzukommen. Über Art und Umfang der erforderlichen Mittel sollte Einvernehmen mit dem Datenschutzbeauftragten hergestellt werden. Sodann sollte die Behördenleitung darauf hinwirken, daß der Datenschutzbeauftragte seine Überwachungs- und Mitwirkungspflichten auch tatsächlich erfüllt. Ihm sollten nur solche weiteren Aufgaben auf dem Gebiet des Datenschutzes übertragen werden, zu deren Erledigung er personell und sachlich auch tatsächlich in der Lage ist. Es sollte dem Zustand entgegen gewirkt werden, daß die Behördenleitung sich auf eine Überwachungsfunktion des behördlichen Datenschutzbeauftragten verläßt, die dieser tatsächlich gar nicht ausübt

bzw. ausüben kann. Die diesbezüglichen Aufgaben und die Art ihrer Erledigung sollten beschrieben bzw. dokumentiert werden.

Die Umsetzung unserer Verbesserungsvorschläge stellt die Landeshauptstadt Kiel offenbar vor größere Probleme. Sie hat jedenfalls allein für die Ausarbeitung einer ersten Stellungnahme eine Frist von 4 Monaten erbeten. Die praktischen Ergebnisse der Überprüfung können daher erst im nächsten Tätigkeitsbericht dargestellt werden.

6.1.3 **Datenschutzrechtliche Forderungen aus einer Prüfung im Jahr 1989 werden noch immer abgearbeitet**

Auch wenn Forderungen aus Prüfungsmaßnahmen von den datenverarbeitenden Stellen akzeptiert werden, dauert es oft lange, bis die tatsächlichen Konsequenzen in der Praxis aus ihnen gezogen werden. Die Datenzentrale arbeitet noch heute an der Umsetzung einer Kontrolle aus dem Jahre 1989.

Zu denjenigen Prüfungsmaßnahmen, deren Abwicklung einen unverhältnismäßig langen Zeitraum erfordert, gehört auch die Nachschau bei der **Datenzentrale** Schleswig-Holstein aus dem Jahre 1989 (vgl. 14. TB, S. 85). Allerdings kann man in diesem Fall der datenverarbeitenden Stelle keine Untätigkeit vorwerfen. Man mag zwar Zweifel haben, ob die Umsetzung der datenschutzrechtlichen Forderungen und Verbesserungsvorschläge bisher mit dem möglichen Nachdruck erfolgt ist, ob alles nicht etwas zügiger hätte in Angriff genommen werden können. Betrachtet man jedoch das Volumen der sich aus der Überprüfung ergebenden technischen und organisatorischen Veränderungen und den damit verbundenen personellen und finanziellen Aufwand, kann man Verständnis dafür haben, daß die Datenzentrale sich die Entscheidungen reiflich überlegt und – aus ihrer Sicht – die Dinge nicht „über das Knie bricht“.

Wir haben aus diesem Grunde Vorsorge getroffen, daß die Abarbeitung unserer als berechtigt akzeptierten Forderungen über einen so langen Zeitraum hinweg letztlich nicht im Sande verläuft. Mit der Datenzentrale ist vereinbart, daß sie uns halbjährlich über den Fortgang der Arbeiten informiert. Die **diesjährige Bilanz** kann man durchaus als **eindrucksvoll** bezeichnen. Sie umfaßt nicht weniger als 18 Einzelpositionen, in denen die definitive Erledigung, zumindest aber der Fortgang der Arbeiten zur Erledigung eines im Jahre 1990 vereinbarten Maßnahmenkatalogs dargestellt wird. Worum es dabei geht, mag ein Beispiel verdeutlichen: Wir hatten beanstandet, daß der Zugriff der Datenzentrale auf die Kundendaten im Rahmen der Auftragsdatenverarbeitung nicht hinreichend geregelt war. Um dieses Problem mit all seinen Randbedingungen in den Griff zu bekommen, sah sich die Datenzentrale

veranlaßt, nicht weniger als 15 Arbeitsanweisungen zu ändern bzw. völlig neu zu gestalten.

Gleichwohl spricht die Datenzentrale selbst erst von „wesentlichen Fortschritten“ und daß sie erst zu einem späteren Zeitpunkt über den endgültigen Abschluß der Arbeiten unterrichten könne. Aber auch damit wird man aus unserer Sicht die Prüfungsmaßnahme noch nicht „ad acta“ legen können. Zwischen der (positiven) Darstellung, **daß** man etwas getan hat, und dem, **was** tatsächlich inhaltlich realisiert worden ist, bestehen nicht selten signifikante Unterschiede. Auch dies läßt sich durch zwei Beispiele verdeutlichen:

– Leistungsbeschreibungen

Es ist positiv zu bewerten, daß die Datenzentrale für alle automatisierten Verfahren, die sie im kommunalen Bereich anbietet, sogenannte **Leistungsbeschreibungen** erstellt hat, aus denen hervorgehen soll, welche Dienstleistungen sie im einzelnen im Rahmen der Auftragsdatenverarbeitung erbringt und welche Aktivitäten auch weiterhin von ihren Kunden erbracht werden müssen. Es handelt sich dabei nicht nur um eine Schnittstellendefinition, sondern auch um ein Element der rechtswirksamen Auftragserteilung durch die Behörde, weil die Leistungsbeschreibungen Bestandteil der Verträge werden. Deshalb erscheint es nicht unproblematisch, wenn in einem Verfahren, mit dessen Hilfe Sozialdaten verarbeitet werden, folgende Formulierungen benutzt werden: „Zur ... Untersuchung unklarer betrieblicher Störungszustände ... sind die dazu befugten Mitarbeiter der Datenzentrale ... berechtigt, ... **bestandsverändernd** auf Wohngelddaten zuzugreifen. Solche bestandsverändernden Zugriffe sind zu dokumentieren und dem Kunden zur Kenntnis zu geben.“ Bestandsveränderungen durch einen Auftragnehmer an Datenbeständen, die einem besonderen Berufs- und Amtsgeheimnis unterliegen, dürften eine der „brisantesten“ denkbaren Aktionen eines Auftragnehmers sein. Deshalb wäre gerade hier eine bis ins kleinste Detail ausformulierte Regelung erforderlich gewesen: Wie werden die entsprechenden Weisungen erteilt? Wie wird dokumentiert? Welche Unterlagen erhält der Kunde? usw.

An einer anderen Stelle wird festgelegt: „Ausschußmaterial wird unter Beachtung der notwendigen Sicherungsmaßnahmen von der Datenzentrale vernichtet. Die Datenzentrale ist berechtigt, im Rahmen dieser Sicherungsmaßnahmen hiermit auch Subunternehmer zu beauftragen“. Dies kann bedeuten, daß die Schredderung von Wohngeldbescheiden nicht im Haus der Datenzentrale, sondern bei einem privaten Unternehmer stattfindet. Die Bescheide gehen diesem Unternehmen gezwungenermaßen in lesbarer Form zu, bevor aus ihnen Papierschnipsel werden. Eine derartige Einschaltung nichtöffentlicher Auftragnehmer unterliegt besonders strengen Regelungen des SGB X. Auf diese rechtliche Gegebenheit wird in den Leistungsbeschreibungen der Datenzentrale nicht eingegangen.

– **Freigabe von automatisierten Verfahren im kommunalen Bereich**

Nachdem der Innenminister im Jahre 1990 bezüglich des Tests und der Freigabe von Programmen und Verfahren im Rahmen des Einwohnerinformationssystems unseren wiederholten Forderungen nachgekommen ist und durch eine entsprechende Weisung an die Meldebehörden für ein datenschutzrechtlich befriedigendes Verfahren gesorgt hat, ist dies von der Datenzentrale in ihrer Publikation für ihre Kunden (Informationsbrief 3/92) als „positiv“ für die Qualität der eingesetzten Programme bezeichnet worden. Auch in dem o.a. Sachstandsbericht der Datenzentrale für das Jahr 1992 wird diese Umstellung als Fortschritt gewürdigt. Es muß dabei aber erwähnt werden, daß es neben dem Einwohnerinformationssystem eine Vielzahl weiterer Verfahren gibt, für die das Test- und Freigabeverfahren noch nicht umgestellt ist. Noch verlassen sich die Kommunen hier auf eine Überprüfung der Richtigkeit der Programme durch ein Fachgremium, die in einer hinreichend wirksamen Form gar nicht stattfindet.

Für uns ergibt sich aus derartigen Gegebenheiten die Konsequenz, größere Prüfungsmaßnahmen grundsätzlich um die Komponente „Analyse und Bewertung der tatsächlich getroffenen Maßnahmen zur Verbesserung des Datenschutzes“ zu ergänzen. Dies wird auch in bezug auf die Prüfung bei der Datenzentrale geschehen.

6.2 Beachtung der neuen Sicherheits- und Ordnungsmäßigkeitsvorschriften

6.2.1 Alle warten auf die Datensicherungsverordnung

Viele Behörden würden verbindliche Vorschriften zur Einhaltung eines bestimmten Datensicherungs-niveaus durchaus begrüßen. Die Verordnung zur Datensicherung sollte deshalb bald verabschiedet werden.

Mit dem Hinweis, daß die Landesregierung „jetzt in der Pflicht“ sei, haben wir im letzten Tätigkeitsbericht (vgl. 14. TB, S. 72) darauf aufmerksam gemacht, daß sie durch das seit Anfang 1992 geltende Datenschutzgesetz verpflichtet ist, den datenverarbeitenden Stellen im Lande auf dem Verordnungswege nähere Weisungen zu den Themen „**Datensicherheit**“ und „**Ordnungsmäßigkeit der Datenverarbeitung**“ zu erteilen. Durch die frühzeitige Vorlage eigener Regelungsvorschläge und intensive Mitarbeit in vorbereitenden Arbeitsgruppen haben wir zudem versucht, den Gang des Verfahrens zu beschleunigen.

Nach einjähriger Erfahrung mit dem Versuch der Neuregelung der „technischen und organisatorischen Maßnahmen“ im Landesdatenschutzgesetz ist festzustellen, daß eine zügigere Behandlung der Angelegenheit angezeigt ist. Die Tatsache, daß

die von den datenverarbeitenden Stellen schlicht als „Datensicherungsverordnung“ bezeichnete Rechtsverordnung noch nicht beschlossen ist, führt nämlich bei vielen Behörden zu einem faktischen **Stillstand** bei der **Fortentwicklung der Datensicherungsmaßnahmen**. Wer will es einem EDV-Leiter auch verdenken, wenn er im Augenblick Entscheidungen über Investitionen in dem Bereich Datensicherheit vor sich herschiebt, weil er fürchtet, nach Inkrafttreten der Verordnung andere Prioritäten setzen zu müssen.

Wir können eine solche „Verzögerung“ natürlich grundsätzlich nicht akzeptieren. Machen wir etwa im Rahmen von Prüfungen Verbesserungsvorschläge, wird stets auch nach Prioritäten gefragt. Dabei ist es zur Zeit durchaus nicht einfach, die Frage zu beantworten: „Und was ist, wenn die Verordnung in Kraft tritt, und dann kein Geld mehr da ist für die Maßnahmen, die durch sie bindend vorgeschrieben werden?“

In diesen Gesprächen zeigt sich zudem, daß die Datenverarbeiter offensichtlich mehr erwarten, als der Innenminister derzeit zu regeln plant. Dies mag ein Beispiel verdeutlichen: Unter Fachleuten ist es unbestritten, daß die Probleme in der Software-Pflege nur durch detaillierte und einheitliche **Dokumentationsvorschriften** zu lösen sind. Deshalb werden derartige Regelungen auf dem Verordnungswege als selbstverständlich vorausgesetzt. Diskutiert wird eigentlich nur über die Notwendigkeit, für die bereits bestehenden Programme und Verfahren „großzügige“ **Übergangsregelungen** zu schaffen, damit für die Behebung der „Sünden der Vergangenheit“ nicht Personal gebunden wird, das man für die Fortführung der aktuellen Projekte benötigt.

Die schwierige Situation, in der sich der Innenminister befindet, weil es für eine derartige Verordnung bundesweit keine Musterlösung gibt, soll nicht verkannt werden. Wir werden deshalb im nächsten Jahr unser Engagement für den raschen Erlass der Verordnung weiter verstärken.

6.2.2 Datenverarbeitende Stellen versäumen Übersendung der Dateibeschreibungen

Obwohl die datenverarbeitenden Stellen bei der Meldung von Dateien, in denen personenbezogene Daten gespeichert sind, durch Technikeinsatz entlastet werden, kommen viele Behörden ihren Meldepflichten nicht nach.

Auch das neue Datenschutzgesetz sieht vor, daß die datenverarbeitenden Stellen für alle Dateien, in denen personenbezogene Daten gespeichert sind, **Dateibeschreibungen** zu erstellen haben. Diese Dateibeschreibungen sind bei der Aufnahme der Verarbeitung in Kopie an uns zu übersenden und regelmäßig zu aktualisieren. Wir führen auf der Grundlage der übersandten Unterlagen eine Dateienübersicht, in die jede Person Einsicht nehmen kann. Die **Dateienübersicht** wird von uns mindestens alle fünf Jahre in geeigneter Weise veröffentlicht.

Da sich die Art und der Umfang der Angaben in den Dateibeschreibungen nach altem und nach neuem Recht nicht vollständig decken, hätten eigentlich auch diejenigen Dateien neu gemeldet und registriert werden müssen, die bereits seit Jahren benutzt werden. Es handelt sich dabei um eine Größenordnung von **mehreren tausend Dateien**.

Unter Berücksichtigung der Schwierigkeiten, die beim Aufbau des bisherigen Dateienregisters zu überwinden waren, galt es, ein Verfahren zu entwickeln, das die datenverarbeitenden Stellen soweit wie möglich entlastet, gleichzeitig aber zu einem Register führt, das im Hinblick auf die Vollständigkeit und Richtigkeit der erfaßten Dateien diese Bezeichnung auch verdient.

Die Dateienübersicht soll in Form einer Datenbank auf dem in der Dienststelle bereits für andere Zwecke installierten Rechnersystem geführt werden. Zu diesem Zweck wurden **spezielle Erhebungsvordrucke** für alle manuellen Dateien und für alle neuen automatisierten Dateien entwickelt. Mit ihnen werden auch ergänzende Angaben erfaßt, die für die Klassifizierung und Gewichtung der Dateien im Hinblick auf die spätere Veröffentlichung von Bedeutung sind.

Als ein besonderer Vorteil dieser Datenbanklösung und als ein Service für die datenverarbeitenden Stellen ist die Tatsache anzusehen, daß es uns möglich sein wird, die bisherigen Meldungen weitgehend in den neuen Bestand zu übernehmen. Den Behörden werden dann sukzessiv in der Form von „**Kontoauszügen**“ die Dateibeschreibungen zum Zweck der **Kontrolle der Aktualität und der Ergänzung** der fehlenden Eintragungen übersandt. Das gilt auch für die standardisierten Dateibeschreibungen der Datenzentrale. Die Maßnahme wird sich in Abhängigkeit von der personellen Kapazität zwar über einen längeren Zeitraum erstrecken, sie entlastet die datenverarbeitenden Stellen aber erheblich.

Im September haben wir die Behörden durch eine Veröffentlichung im Amtsblatt Schleswig-Holstein (Nr. 40, S. 674) auf die neue Rechtslage und Verfahrensweise aufmerksam gemacht. Bis zum Ende des Jahres sind daraufhin ein knappes Dutzend Meldungen auf der Grundlage des neuen LDSG eingegangen. Es hätten mehrere Hundert sein müssen, da alle nicht automatisierten Dateien nachzumelden sind und seit Inkrafttreten des neuen Landesdatenschutzgesetzes sicherlich viele neue EDV-Dateien entstanden sind. Es ist zu hoffen, daß die datenverarbeitenden Stellen unseren Service nicht dahin gehend mißverstanden haben, daß sie gar nichts mehr zu veranlassen hätten.

6.2.3 Geräteverzeichnisse – mehr als bloße Formalität?

Konfigurationspläne und Programmverzeichnisse sind als rechtliche Voraussetzungen für die Inbetriebnahme informationstechnischer Systeme anzusehen.

Professionelle Datenverarbeiter haben sich verwundert gezeigt, als sie im Entwurf des neuen Landesdatenschutzgesetzes die Bestimmung fanden, die datenverarbeitenden Stellen hätten ein **Geräteverzeichnis** zu führen, aus dem sich ergibt, wo welche Computer installiert sind, welche Betriebssysteme und Programme benutzt werden und wie die Geräte gesichert sind. Sogenannte Konfigurationspläne seien doch eine Selbstverständlichkeit, da bedürfe es doch keiner besonderen gesetzlichen Regelung.

Nach unseren **Prüferfahrungen** ist es aber selbst nach Einführung der gesetzlichen Regelung bei mittleren Behörden die Regel, bei großen Datenverarbeitern nicht unbedingt eine Ausnahme, daß auf der Ebene der Amts- und Verwaltungsleitung kein Überblick über die aktuelle Konfiguration besteht. Meistens ist lediglich bekannt und dokumentiert, welcher Gerätebestand geplant war. Die tatsächliche Realisierung beziehungsweise die Fortschreibung des EDV-Konzeptes bleibt den Amts- und Behördenleitern offenbar häufig verborgen. Hierin ist die Ursache vieler Datensicherungsmängel zu sehen. Standortänderungen, Nutzungsänderungen, Aufgabenerweiterungen usw., führen fast immer dazu, daß ursprünglich funktionierende Sicherheitskonzepte ihre Wirkung verlieren.

Wir setzen uns daher mit Nachdruck dafür ein, daß die Erfassung der eingesetzten Hard- und Software in dem Geräteverzeichnis generell als **rechtliche** Voraussetzung für den Betrieb automatisierter Verfahren angesehen wird. Nur auf diese Weise wird man der Verbreitung von sicherheitsbedrohenden Viren und der unbefugten Nutzung von Computersystemen entgegenwirken können. Dies haben die Erfahrungen in der sicherheitsempfindlichen Groß-EDV eindeutig bewiesen. Dieser Problembereich wird deshalb bei den Prüfungen in der nächsten Zeit als ein besonderer Schwerpunkt berücksichtigt.

6.2.4 Kein Datenschutz beim Funkverkehr?

Eine neue EG-Regelung erleichtert das Abhören des Funkverkehrs. Die Behörden, die auf dem Funkwege kommunizieren, müssen durch zusätzliche technische und organisatorische Maßnahmen die Datensicherheit gewährleisten. Hierzu ist die Verschlüsselung ein geeignetes Mittel.

Als vor einigen Monaten in der Presse berichtet wurde, daß der Bundespostminister im Zuge der Harmonisierung von Rechtsvorschriften in den EG-Mitgliedsstaaten beabsichtige, die Benutzung von Geräten zu „liberalisieren“, die geeignet sind, auch den **Funkverkehr abzuhören**, gelangte ein Thema in die datenschutzrechtliche Diskussion, das wir bereits vor mehr als zehn Jahren (vgl. 3. TB, S. 13) problematisiert hatten. Wenn Behörden untereinander oder mit Bürgern kommunizieren, dann geschieht das in der Regel durch den Versand verschlossener Briefumschläge oder telefonisch. Man geht in beiden Fällen davon aus, daß der Inhalt der ausgetauschten Informationen dem unbefugten Zugriff Dritter entzogen ist,

die **Amtsverschwiegenheit** bzw. die **besonderen Berufs- und Amtsgeheimnisse** mithin gewahrt bleiben.

Diejenigen Behörden, die mit ihren Mitarbeitern bzw. mit Dritten im Wege des Funkverkehrs kommunizieren, das sind z.B. die **Polizei**, die **Rettungsleitstellen** und die **Feuerwehr**, nehmen seit jeher in Kauf, daß die so ausgetauschten Informationen nicht in gleichem Maße geheimgehalten werden können. Bastlern und anderen interessierten Personen war es zwar untersagt, gleichwohl aber mit einem gewissen technischen Aufwand möglich, die entsprechenden Frequenzen abzuhören, um z.B. an polizeiliche Daten zu gelangen. Beispiele hierfür hat es genug gegeben. Die größte Publizität erlangte vor einigen Jahren der vollständige Mitschnitt und die systematische Auswertung des polizeilichen Funkverkehrs während der Studentenunruhen in Göttingen.

Zur Rechtfertigung/Entschuldigung dieser **Sicherheitslücke** haben sich die betreffenden Behörden bisher immer darauf berufen, daß der Besitz und die Benutzung derartiger Geräte unzulässig sei, und daß man sich gegen strafbare Handlungen nicht hundertprozentig schützen könne. Diese Argumentation greift spätestens seit der Neuregelung zu kurz. Die Tatsache, daß künftig praktisch jeder, der nur hinreichend neugierig ist, die Möglichkeit hat, die betreffenden Frequenzen mit handelsüblicher Technik abzuhören, zwingt zu Reaktionen derjenigen, die zur Wahrung der **Datensicherungs- und Verschwiegenheitsvorschriften** verpflichtet sind.

Eine adäquate Maßnahme im Sinne der datenschutzrechtlichen „**Transportkontrolle**“ wäre die Verschlüsselung des Funkverkehrs der o.a. Behörden. Dies ist kein technisches, sondern „nur“ ein finanzielles Problem. Immerhin sind Technikinvestitionen in der Größenordnung von mehreren Millionen DM (nach derzeitigem Preisniveau) zu erwarten. Gleichwohl kann das Kostenargument nicht auf Dauer die Rechtfertigung dafür sein, daß von der Realisierung der **Verschlüsselungstechnik** abgesehen wird. Immerhin geht es beispielsweise beim polizeilichen Funkverkehr um sensible personenbezogene Daten, von den Sicherheitsaspekten ganz zu schweigen. Ob es um das Ergebnis einer Abfrage in der Fahndungs- oder einer sonstigen polizeilichen Datei geht, die Beorderung eines Funkstreifenwagens zum Einsatzort, die ersten, per Funk übermittelten Berichte vom „Tatort“: In jedem Fall kann es zur Übermittlung und – unter den gegebenen Umständen – Offenbarung von besonders schützenswerten personenbezogenen Daten kommen.

Bis die Verschlüsselungstechnik angeschafft ist, müssen bereits jetzt Maßnahmen zur **Reduzierung des Risikos** ergriffen werden. Eine Einschränkung der unbefugten Offenbarung (hierum handelt es sich, wenn eine Behörde nicht unterbindet, daß man ihren Funkverkehr mithört) läßt sich z.B. dadurch erreichen, daß außer den unvermeidlichen personenbezogenen Angaben (Name, Anschrift usw.) alle „inhaltlichen“ Merkmale (Grund der Anfrage, Inhalt der Antwort usw.) in Form von

Schlüsselwerten übermittelt werden. Den „Mithörern“ wird auf diese Weise nur bekannt, daß eine bestimmte Person Kontakt mit der Polizei, dem Rettungsdienst usw. hat. Es bedürfte jedoch einer systematischen Recherche, um herauszufinden, in welchem Kontext diese Information steht. In anderen Fällen, wenn beide Funkpartner ohnehin wissen, von wem die Rede ist, kann auf die Nennung des Namens verzichtet werden.

6.3 Aus der Arbeit der IT-Kommission des Landes und der Automationskommission der Kommunen

6.3.1 Musterregelung für den Einsatz privater Personalcomputer

Private PC dürfen für dienstliche Zwecke nur eingesetzt werden, wenn die Behörden die Verfügungsgewalt über die Geräte besitzen. Hierfür hat die IT-Kommission Richtlinien erarbeitet.

Seit Jahren wird heftig darüber diskutiert, ob und ggf. unter welchen Voraussetzungen Mitarbeiter in den Behörden ihre **privaten PC** für **dienstliche Zwecke** benutzen dürfen. Von den Datenverarbeitern werden als Gründe für die Genehmigung derartiger Privatinitiativen u.a. genannt: Erhöhte Motivation der Mitarbeiter, bessere Akzeptanz für den Umgang mit der Informationstechnik, Erhöhung der Arbeitsplatzeffektivität, Ausgleich fehlender finanzieller Mittel zur sachgerechten technischen Ausstattung der Arbeitsplätze. Dagegen sprechen aus datenschutzrechtlicher Sicht: Fehlende Kontrollmöglichkeiten durch die Behörden, somit Verstoß gegen die datenschutzrechtliche Überwachungspflicht, erhöhte Sicherheitsrisiken, fehlende Dokumentation, Unmöglichkeit einer wirkungsvollen Revision.

Da trotz dieser Vorbehalte Behörden den Einsatz privater PC für dienstliche Zwecke tolerieren, hat sich die IT-Kommission des Landes veranlaßt gesehen, in einer „Richtlinie für die Nutzung privater Datenverarbeitungsanlagen in Diensträumen“ die **Rahmenbedingungen** abzustecken, unter denen die ökonomischen Notwendigkeiten sowie die datenschutzrechtlichen und die technisch-organisatorischen Erfordernisse „unter einen Hut zu bringen“ sind.

Wir haben an den Beratungen dieser Richtlinie mitgewirkt. Sie geht von dem Grundsatz aus, daß die Benutzung privater Datenverarbeitungsanlagen in Diensträumen grundsätzlich untersagt ist. Im Einzelfall kann die Benutzung für einen begrenzten Zeitraum gestattet werden, wenn u.a. folgende Bedingungen erfüllt sind:

- Vertragliche Regelung zwischen dem Eigentümer der Datenverarbeitungsanlage und der Behörde auf der Grundlage eines der Richtlinie beigefügten **Mustervertrages**,
- Verpflichtung, nur **genehmigte** Hard- und Software einzusetzen,

- Gewährleistung einer „normalen Aktenführung“ durch eine umfassende **Dokumentation** der Arbeitsergebnisse,
- Sicherstellung, daß keine **Datenbestände** angelegt werden, von denen die Dienststelle nichts weiß,
- Möglichkeit für die Behörde, jederzeit ihre **uneingeschränkte Verfügungsgewalt** über alle dienstlichen Daten ausüben zu können; daher müssen Eigentumsvorbehalte Dritter an der Hardware ausgeschlossen sein, dürfen Verschlüsselungscodes nur mit Einwilligung der Behörde benutzt werden.
- Gewährleistung der **Mitbestimmungs- und Beteiligungsrechte** des Personalrates und der Gleichstellungsbeauftragten.

Sowohl die Vorgehensweise wie auch das Ergebnis der Arbeit der IT-Kommission sind bemerkenswert. Die geschaffene Richtlinie reagiert mit konkreten Lösungsvorschlägen auf eine aktuelle Problemstellung. Sie drängt die Behörden durch die Praxisnähe der in ihr enthaltenen Regelungen (z.B. durch einen Mustervertrag) zum Handeln.

6.3.2 **Mindestanforderungen an die Verfahrensdokumentation in Kraft**

Mit den Mindestanforderungen an die Dokumentation von informationstechnischen Maßnahmen ist eine Grundlage für eine landesweite Standardisierung geschaffen worden.

Die Diskussionen über die Notwendigkeit und die Art der Dokumentation von einzelnen Computerprogrammen und komplexen automatisierten Verfahren sind vermutlich so alt wie die Datenverarbeitung in der öffentlichen Verwaltung, in jedem Fall aber so alt, wie das Datenschutzrecht. Wer die **ordnungsgemäße Anwendung** der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, nach den Regeln des Landesdatenschutzgesetzes zu überwachen hat, muß in einer Programm- und Verfahrensdokumentation auch nachlesen können, was als „der Ordnung gemäß“ anzusehen ist.

Es hat zwar in früheren Verwaltungsanweisungen und in den Anforderungen der Rechnungshöfe Versuche gegeben, derartige **Dokumentationen** zu standardisieren, damit sachverständige Dritte in die Lage versetzt werden, in angemessener Zeit die Inhalte und die Zielrichtung der betreffenden automatisierten Verfahren nachzuvollziehen. Das hat aber nicht dazu geführt, daß alle Behörden im Lande die von ihnen eingesetzte Software konsequent dokumentieren und noch viel weniger dazu, daß die benutzten Dokumentationsmethoden ein Mindestmaß an Ähnlichkeit aufweisen (vgl. 14. TB, S. 75).

Deshalb haben wir die Initiative der IT-Kommission, (neue) „Mindestanforderungen an die Verfahrensdokumentation“ auf der Grundlage der „IT-Verfahrensregelung“ zu schaffen, be-

grüßt und unterstützt. In der nunmehr von der **IT-Kommission** beschlossenen **Richtlinie** werden erfreulicherweise eine Reihe unserer datenschutzrechtlichen Forderungen berücksichtigt. So wird z. B. bestimmt,

- daß nicht nur die fertigen Programme und Verfahren, sondern auch deren Grundlagen, nämlich die Ergebnisse der **Vor- und Hauptuntersuchungen** als „Beschreibung der Aufgabenstellung“ zu dokumentieren sind,
- daß die nach dem Landesdatenschutzgesetz erforderlichen **Dateibeschreibungen** in der Form von logischen und physischen Datenmodellen Bestandteil der Dokumentation sind,
- daß für jedes einzelne Programm ein **Logbuch** zu führen ist, aus dem sich ergibt, ab wann welche Programmversion eingesetzt worden ist,
- daß jede Veränderung am Programmcode zu einer **neuen Programmversion** führen muß,
- daß **nachvollziehbar** sein muß, welche Programme in welchen Verfahren eingesetzt werden,
- daß die **Ergebnisse der Tests** so aufzubewahren sind, daß Vergleiche zwischen den erwarteten und den tatsächlichen Ergebnissen möglich sind,
- daß für jede Verfahrensversion die Freigabe zum Einsatz in Form einer **Freigabebescheinigung** nachgewiesen werden muß.

Die vorstehenden und die in der Richtlinie enthaltenen weiteren Mindestanforderungen verzichten bewußt auf die Festlegung von „Formalitäten“ (wie Vordruckmuster usw.), sondern definieren statt dessen **Zielvorgaben**. Dies dürfte dem praktischen Einsatz in den verschiedensten Verwaltungsbereichen dienlich sein. Wichtig ist jetzt, daß den Richtlinien das Maß an Verbindlichkeit zukommt, das erforderlich ist, um ihre Beachtung bei allen Datenverarbeitungsstellen im Lande obligatorisch zu machen. Die Verordnung zu § 7 LDSG (vgl. Tz. 6.2.1) sollte daher die Grundüberlegungen dieser Richtlinie übernehmen und sie bezüglich ihrer Detailregelungen für allgemeinverbindlich erklären.

6.3.3 Die IT-Verfahrensregelung wird nicht immer beachtet

Bei der Entwicklung automatisierter Verfahren sind nach der IT-Verfahrensregelung Datenschutz- und Datensicherungsfragen rechtzeitig zu lösen. Die Praxis sieht häufig anders aus.

Auf unsere Initiative enthält die IT-Verfahrensregelung des Landes die Verpflichtung für die Behörden, bereits in einem frühen Stadium der Entwicklung automatisierter Verfahren eine „Darstellung der vorgesehenen Maßnahmen zur **Verfahrenssicherheit und zum Datenschutz**“ vorzunehmen. Diese Konzeptionen sind dann der IT-Kommission als Bestandteil der Beschlußunterlagen vorzulegen, aufgrund derer sie ihre

gutachterliche Stellungnahme bezüglich der Realisierung der Verfahren abgibt.

Leider war in der Vergangenheit des öfteren festzustellen, daß selbst bei datenschutzrechtlich durchaus nicht unproblematischen Automationsvorhaben unter der betreffenden Textziffer der Beschlußvorlagen „**Platzhalter**“ wie z. B. „... werden zu einem späteren Zeitpunkt festgelegt“ zu finden sind. Wir haben in den Sitzungen der IT-Kommission stets auf diesen Mangel aufmerksam gemacht. Gleichwohl hat sich die Kommission bisher noch nicht veranlaßt gesehen, deshalb ein positives Votum zu verweigern und eine Ergänzung der vorgelegten Planungsunterlagen zu fordern.

Sollten sich die datenverarbeitenden Stellen hierdurch ermuntert sehen, entgegen den Bestimmungen der IT-Verfahrensregelung die Lösung der Datenschutz- und Datensicherheitsfragen bei der Realisierung von Automationsvorhaben **regelmäßig sehr spät**, unter Umständen zu spät, in Angriff zu nehmen, entstehen nicht nur gravierende Rechtsprobleme (vgl. Tz. 4.9.2), sondern verstärkt auch Änderungskosten (vgl. z.B. 13. TB, Sn. 8 und 49).

6.3.4 Richtungweisende Empfehlungen der Automationskommission der Arbeitsgemeinschaft der kommunalen Landesverbände

Im Juli 1991 hat die Automationskommission der Arbeitsgemeinschaft der kommunalen Landesverbände „Empfehlungen zur Weiterentwicklung der technikunterstützten Informationsverarbeitung in den Kommunalverwaltungen Schleswig-Holsteins“ veröffentlicht, die aus datenschutzrechtlicher Sicht in vielen Punkten als richtungweisend angesehen werden können.

Die Automationskommission sieht (wie auch die Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung) für die Entwicklung der technikunterstützten Informationsverarbeitung drei konzeptionelle Schwerpunkte.

– Infrastrukturansatz

Jeder Verwaltung wird empfohlen, eine informationstechnische Infrastruktur nach einheitlichen Grundsätzen fachbereichsübergreifend zu planen und zu verwirklichen. Sie müsse das von der Verwaltung gewollte Entscheidungsergebnis sein, „das aufgrund von immer wieder notwendigen Organisationsüberlegungen und Wirtschaftlichkeitsbetrachtungen im Rahmen eines dynamisch fortzuschreibenden **Technologiekonzeptes** ganzheitlich realisiert, ständig weiterentwickelt und in der Routine verlässlich betrieben wird“.

Mit dem Infrastrukturansatz werde die **Dezentralisierung** der Technik gefördert. Dies bedeute für die Verwaltung, daß Systemverantwortliche die sich aus dem laufenden Betrieb auf der Ebene des Arbeitsplatzes wie auch der Verwaltungs-

rechnerebene ergebenden Bedieneraktivitäten beherrschen müßten. Der Umfang des Know-hows in der Verwaltung sei so weit aufzubauen, daß die **Systemverantwortlichen** alltägliche Probleme einschließlich der Einarbeitung und Schulung neuer Mitarbeiter selbständig erledigen könnten. Es sei eine sinnvolle Abgrenzung zu Spezialistenwissen in zentralen Stellen der eigenen Verwaltung, in der Datenzentrale beziehungsweise bei Herstellern zu finden und dort in Anspruch zu nehmen.

– **Verwaltungsreformansatz**

Der Übergang der Verwaltung in eine weitreichende technische Unterstützung der Verwaltungsarbeit könne nur als umfassend anzulegender **Modernisierungs- und Erneuerungsprozeß** verstanden und behandelt werden. Dieser Prozeß sei gerichtet auf eine Produktivitätssteigerung der Verwaltung und insbesondere auf die Veränderung ihrer inneren und äußeren Strukturen.

Bei der Planung derartiger Vorhaben seien die möglichen Folgen des Ausfalls und nicht ordnungsgemäßer, insbesondere mißbräuchlicher Nutzungen von technischen Einrichtungen zu prüfen. Die festgestellten **Risiken** und **Auswirkungen** seien unter Beachtung der Wirtschaftlichkeit durch organisatorische, personelle und technische Maßnahmen zu begrenzen. Wenn dies nicht möglich sei, müsse von der Realisierung des betreffenden Vorhabens abgesehen werden.

Zudem seien die **rechtlichen Rahmenbedingungen** zu beachten. Hierzu gehörten insbesondere:

- die Tarifvorschriften, insbesondere der Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informations- und Kommunikationstechnik,
- Vorschriften des Arbeitsschutzes, insbesondere über die Gestaltung von Bildschirmarbeitsplätzen,
- die Gemeindeordnung und das kommunale Finanz- und Kassenrecht,
- die Bestimmungen zur Ordnungsmäßigkeit von Verfahrenen,
- die Bestimmungen des Datenschutzrechts sowie
- die personalvertretungsrechtlichen Belange und eventuelle Mitbestimmungsrechte.

Beim Technikeinsatz seien Vorkehrungen zur Gewährleistung der Vollständigkeit, Richtigkeit und Aktualität der zu verarbeitenden Daten sowie ordnungsgemäßer und fachlich fehlerfreier Verfahrensabläufe (Daten- und Verfahrenssicherheit) zu treffen.

– **Sozialverträglichkeitsansatz**

Der Übergang in die technikerunterstützte Informationsverarbeitung sei ein langfristiger **sozialer Gestaltungsprozeß**.

Die Nutzenpotentiale für den Reformansatz korrespondierten mit den Gefährdungspotentialen für die Mitarbeiter, für das soziale System Verwaltung und für die Gesellschaft. Der sozialverträglichen Technikeinführung müsse deswegen aus personalwirtschaftlicher, organisatorischer, rechts- und gesellschaftspolitischer sowie ökonomischer Sicht die gleiche Aufmerksamkeit und Sorgfalt zugewendet werden wie dem Infrastruktur- und dem Reformansatz. Sie sei anwendungsfreundlich, arbeitsangemessen und im Rahmen von tätigkeits- sowie technikorientierten Perspektiven zu planen und einzurichten. Insbesondere sollten die Beschäftigten nach angemessener Einarbeitungszeit aufgabengerecht und effizient mit den Geräten und Verfahren arbeiten können. Auf kurze Rüst- und Antwortzeiten sowie Fehlertoleranz, weitgehende Selbstbeschreibungsfähigkeit und leichte Bedienbarkeit sei bei der einzuführenden Hard- und Software Wert zu legen. Bei der Arbeitsplatzgestaltung sei auf ergonomische Anforderungen, die Möglichkeit von Belastungswechseln und die Einhaltung von Bildschirmpausen zu achten.

Wir hatten erwartet, daß derartig grundlegende und zutreffende Aussagen der Automationskommission zu einer nachhaltigen Diskussion innerhalb der Kommunen und zu **Konsequenzen** hinsichtlich des Hard- und Software-Angebotes der Datenzentrale und anderer Dienstleister auf diesem Gebiet führen würden. 18 Monate nach Veröffentlichung der Empfehlungen ist aber zu vermuten, daß dieses Papier in vielen Behörden offenbar „zu den Akten“ verfügt worden ist.

Weder sind wir im Rahmen von Prüfungen und Informationsbesuchen auf diese Thematik angesprochen worden, noch haben wir feststellen können, daß die Kommunen ihre Planungen und Realisierungen unter dem Eindruck der Empfehlungen in entscheidender Weise neu ausgerichtet haben. Wir werden bei künftigen Prüfungen im kommunalen Bereich die vorgenannten Grundsätze als Maßstab benutzen, um mit dazu beizutragen, daß die Grundlagen der Automationskommission auch ihren Niederschlag im täglichen Verwaltungshandeln finden.

6.4 Was IT-Führungskräfte wissen sollten

Der Ausbildungsbedarf für IT-Führungskräfte ist unbestritten. Zur Zeit fehlen noch die Konzepte und Träger für entsprechende Seminare.

In unserem 14. Tätigkeitsbericht (S. 78) haben wir gefordert, daß sich die IT-Kommission des Landes, die Arbeitsgemeinschaft der kommunalen Landesverbände, die Datenzentrale und die Hersteller und Vertreiber von Computersystemen an einen Tisch setzen sollten, um ein praktikables Konzept für die Vermittlung der erforderlichen Sachkunde für diejenigen Mitarbeiter der öffentlichen Verwaltung, die für den Einsatz informationstechnischer Systeme die Verantwortung tragen, zu entwickeln. Zu einer gemeinsamen Erörterung der Problema-

tik mit allen beteiligten Stellen ist es im abgelaufenen Jahr noch nicht gekommen. In vielen Gesprächen haben wir aber eine **breite Zustimmung** zu einem Vorschlag gefunden, in dem wir unsere Vorstellungen über die Ausbildungsstrukturen für IT-Führungskräfte über die rein datenschutzrechtlichen Aspekte hinaus zusammengefaßt haben.

Nach unseren Erfahrungen ist davon auszugehen, daß die angehenden IT-Verantwortlichen, aber auch viele Mitarbeiter, die bereits seit Jahren die Verantwortung tragen, i. d. R. nur geringe bzw. fragmentarische Vorkenntnisse auf dem Gebiet der Planung, Realisierung und Handhabung von informationstechnischen Systemen besitzen. Deshalb dürfte die Vermittlung der erforderlichen Lerninhalte insgesamt mindestens eine **vierwöchige Ausbildung** erforderlich machen. Um für Mitarbeiter mit Vorkenntnissen in Teilbereichen diese Zeitdauer verkürzen zu können und um die praktische Durchführung der Ausbildung möglichst flexibel zu handhaben, sollte sie in vier selbständige Seminare aufgegliedert sein. Die Reihenfolge der Seminare sollte beliebig gewählt werden können. Dabei bietet sich folgende **Themengliederung** an:

- Informatik/Informationstechnik
- Planung und Realisierung von IT-Systemen
- Rechtsvorschriften zur Datenverarbeitung und zum Datenschutz
- Revision/Kosten-Nutzen-Analysen

Aus unserer Sicht müßte den IT-Führungskräften zu den einzelnen Themenbereichen im wesentlichen folgendes Wissen vermittelt werden:

- **Bereich „Informatik/Informationstechnik“**
 - Grundlagen der Informatik,
 - grundsätzliche Unterschiede zwischen den verschiedenen Rechnerarchitekturen, die aktuell in der Verwaltung eingesetzt werden,
 - künftige Entwicklungen in der Kommunikations- und Informationstechnik,
 - Grundzüge der verschiedenen Betriebssysteme, Programmiersprachen und Datenbanken,
 - rechtliche Bedeutung und Methoden der Programm- und Verfahrenstests und -freigabe,
 - allgemeine Sicherheitsüberlegungen im Zusammenhang mit den Begriffen „Integrität“, „Vertraulichkeit“ und „Verfügbarkeit“,
 - Manipulationsmöglichkeiten an und mit IT-Systemen.
- **Bereich „Planung und Realisierung von IT-Systemen“**
 - Rechtliche Problemstellungen beim Verwaltungshandeln unter Einsatz von IT-Systemen,
 - aufbauorganisatorische Änderungen und Maßnahmen bei der Umstellung von der konventionellen auf die automatisierte Datenverarbeitung.

- Auswirkung des Technikeinsatzes auf die Ablauforganisation einer Behörde,
 - Beteiligungsrechte der Mitarbeiter und des Personalrates nach dem Mitbestimmungsgesetz,
 - Anforderungen an die Arbeitsplatzergonomie, arbeits- und tarifrechtliche Fragen im Zusammenhang mit Bildschirmarbeitsplätzen, Gestaltung von Arbeitsanweisungen,
 - Anforderungen an die Dokumentation von IT-Systemen.
- **Bereich „Rechtsvorschriften zur Datenverarbeitung und zum Datenschutz“**
- Das Recht auf informationelle Selbstbestimmung,
 - das Landesdatenschutzgesetz und sein Verhältnis zum Verwaltungsverfahrenrecht,
 - materielles Datenschutzrecht im Landesdatenschutzgesetz, im Sozialgesetzbuch, im Polizeirecht, im Verfassungsschutzrecht, im Archivrecht, im Steuerrecht usw.,
 - formale Pflichten der datenverarbeitenden Stelle,
 - Besonderheiten bei der Auftragsdatenverarbeitung,
 - technische und organisatorische Sicherheitsmaßnahmen, Überwachung der ordnungsgemäßen Anwendung der IT-Verfahren,
 - Vergleich des Datenschutzes in der Verwaltung und in der Wirtschaft,
 - strafrechtliche Aspekte des Datenschutzes.
- **Bereich „Revision/Kosten-Nutzen-Analysen“**
- Rechtliche Grundlagen für die Revision und die Kosten-Nutzen-Analysen,
 - Kosten-Nutzen-Betrachtungen für IT-Systeme, computergestützte Anwendungsentwicklung,
 - Dokumentation der einzelnen Entwicklungsphasen von IT-Systemen,
 - haushaltsrechtliche Anforderungen an die Dokumentation von IT-Systemen,
 - Protokollierung von Systemaktivitäten, Schäden durch Ausfall technischer Systeme,
 - Produkthaftung, Amtshaftung, Schadenersatz.

Wir sind bemüht, möglichst bald das Seminar zu dem Thema „Rechtsvorschriften zur Datenverarbeitung und zum Datenschutz“ anbieten zu können und hoffen, daß dies dann eine Signalwirkung für diejenigen Institutionen hat, die in der Lage sind, die Wissensvermittlung auf den anderen Teilgebieten zu übernehmen. Daß der Bedarf seitens der datenverarbeitenden Stellen vorhanden ist, zeigt sich z. B. daran, daß eintägige Veranstaltungen, die wir in Zusammenarbeit mit der Datenzentrale durchführen, sowie andere vergleichbare Veranstaltungen stets über Monate im voraus ausgebucht sind.

Beim **Landesbeauftragten für den Datenschutz**
derzeit erhältliche Publikationen

Datenschutz in Schleswig-Holstein

Text des Landesdatenschutzgesetzes und
des Bundesdatenschutzgesetzes
mit einer erläuternden Einführung

Schleswig-Holsteinischer Datenschutztag '92

Landtagsforum 2. Juni 1992
Dokumentation

Faltblätter „Hat der Bürger Rechte!“

- Die Rechte des Bürgers im Datenschutz
- Was Sie über den Datenschutz wissen sollten
- Die Arbeit des Datenschutzbeauftragten
- Die Pflichten der datenverarbeitenden Stellen

Tätigkeitsberichte

der letzten drei Jahre als Landtagsdrucksache

Tätigkeitsberichte

als Sammlung

Diverse Aufkleber

Info 1

des Bundesbeauftragten für den Datenschutz
Bundesdatenschutzgesetz
– Text und Erläuterung –