SCHLESWIG-HOLSTEINISCHER LANDTAG
13. Wahlperiode

Drucksache 13/2591
17. 03. 95

Bericht

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

**Siebzehnter Tätigkeitsbericht
(Berichtszeitraum: März 1994 bis Februar 1995)**

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

Dr. Helmut Bäumler

Die Landtagsdrucksachen sind fortlaufend und einzeln beim Verlag Schmidt & Klaunig, Ringstraße 19, 24114 Kiel, Fernruf 04 31/6 20 95, zu beziehen.

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

Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/596-3280, Telefax: 0431/596-3300

Der Landesbeauftragte für den Datenschutz:	**Dr. Helmut Bäumler**
Dienstzimmer:	24105 Kiel, 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	
Silke Molt App. 3291	Grundsatzfragen des Datenschutzes Vorbereitung der Sitzungen der Konferenz der Datenschutzbeauftragten Haushalt, Beschaffung Allgemeine Verwaltungsangelegenheiten der Dienststelle Personalangelegenheiten Betreuung der DATENSCHUTZAKADEMIE
Monika Harks App. 3281	Öffentlichkeitsarbeit, Vorbereitung von Veranstaltungen Vorbereitung von Publikationen Fortbildung

Referat LD 2

Eckhard Beilecke App. 3285	
Jürgen von der Ohe App. 3287	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Kataster-, Ausländer-, Kommunal-, Gewerbe-, Bau- und Wirtschaftswesens Datenschutz im Bereich der Parlamentsverwaltung
Holger Brocks App. 3289	Datenschutz im Bereich des Statistik-, Verkehrs-, Umweltschutz-, Planungs-, Zivil- und Katastrophenschutzwesens und im Kultusbereich sowie in Bereichen, für die keine andere Zuständigkeit festgelegt ist, fachübergreifende Fragen der Wissenschaft und der Forschung

Dörte Neumann App. 3297	Dokumentation, Registratur
Heike Reimann App. 3299	Sekretariat
Anke Tuschik App. 3299	

Referat LD 3

Uwe Jürgens App. 3295	
Heiko Behrendt App. 3294	Datenschutz im Bereich der Steuer- und Landwirtschaftsverwaltung sowie innerhalb der Dienststelle des Landesbeauftragten Grundsatzfragen der Datensicherung und der ordnungsgemäßen Anwendung der DV-Programme (§§ 7, 8 LDSG), Prüfung 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
Jan Ziegler App. 3293	Führung und Veröffentlichung der Dateienübersicht (§ 24 LDSG)

Referat LD 4

Herbert Neumann App. 3290	
Gabriele Meyer-Bettyn App. 3286	Datenschutz im Sozial- und medizinischen Bereich
Hans-Jürgen Strasdat App. 3296	Datenschutz im Justiz-, Polizei- und Verfassungsschutzbereich

SIEBZEHNTER 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 1994 bis Februar 1995)

Inhaltsverzeichnis Seite

1.	**Zur Situation des Datenschutzes in Schleswig-Holstein**	9
1.1	Gesetzgebung, Kontrolle und Beratung	9
1.2	Die personelle Ausstattung der Dienststelle	11
2.	**Der Weg in die Computergesellschaft**	12
2.1	Neue Risiken für den Datenschutz der Bürgerinnen und der Bürger	12
2.2	„Modernisierung" der Verwaltung	14
2.2.1	Verzicht auf Datenfriedhöfe	14
2.2.2	Bedingungen für den Computereinsatz	14
2.2.3	Realistische Kostenrechnung	15
2.2.4	Privatisierung verwässert den Datenschutz	16
2.2.5	Abbau obrigkeitsstaatlicher Strukturen	16
2.2.6	Verfassungsrechtliche Grenzen	17
3.	**Datenschutz im Parlament**	18
3.1	Befugnisse parlamentarischer Untersuchungsausschüsse im Lichte des Datenschutzes	18
3.2	Beantwortung parlamentarischer Anfragen durch die Landesregierung	19
3.3	Datenschutzregelung für das Parlament	20
4.	**Datenschutz in der Verwaltung**	22
4.1	**Allgemeine und innere Verwaltung**	22
4.1.1	**Personalwesen**	22
4.1.1.1	Erste Beanstandungen wegen Verletzung des neuen Personalaktenrechts	22

		Seite
4.1.1.2	Wohin mit Arbeitszeitkarten?	23
4.1.1.3	Vergleichsmitteilungen zur Berechnung des Ortszuschlages überflüssig?	23
4.1.1.4	Intime Informationen über Verwandte in Beihilfeanträgen – eine Chance wurde nicht genutzt	24
4.1.1.5	Verarbeitung von Bewerberdaten im Rahmen von internen Personalausleseverfahren	25
4.1.2	**Öffentliche Sicherheit**	26
4.1.2.1	Immer neue Befugnisse für die Polizei – wo bleibt die Sicherheitsdividende?	26
4.1.2.2	Europol	29
4.1.2.3	KpS-Richtlinien in Kraft	31
4.1.2.4	Mangelhafte Kontrollierbarkeit von PED-Abfragen	32
4.1.2.5	COMPAS	33
4.1.3	**Ausländerverwaltung**	33
4.1.3.1	Kein Zwang zur Selbstbezichtigung für Asylbewerber	33
4.1.3.2	Übermittlung von Asylbewerberdaten an die Telekom	35
4.1.3.3	Ausländerzentralregister – nach dem Gesetz nun die Verordnung	36
4.1.3.4	Asylcard	37
4.2	**Umweltschutz**	38
4.3	**Kommunalbereich**	39
4.3.1	Kontrollergebnisse aus den Kommunen	39
4.3.2	Welche personenbezogenen Daten dürfen Gemeindevertreter zur Vorbereitung von Entscheidungen erhalten?	41
4.3.3	Berichtigungsanspruch bei fehlerhafter Darstellung personenbezogener Daten in Gemeindevertretersitzungen	43
4.3.4	Wenn die Kindergärtnerin nach dem Einkommen der Eltern fragt	43
4.3.5	Kontrolle gaststättenrechtlicher Erlaubnisverfahren	45
4.4	**Justizverwaltung**	48
4.4.1	GAST	48
4.4.2	Neue Automationsvorhaben der Justiz	49
4.4.3	Strafakten werden zu lange aufbewahrt	50
4.5	**Steuerverwaltung**	51
4.5.1	Sicherheitsmängel in der Aktenverwaltung der Finanzämter werden zur „unendlichen Geschichte"	51
4.5.2	Kirchensteuermerkmale auf Lohnsteuerkarten – „das haben wir immer so gemacht"	52

		Seite
4.6	**Wirtschaft, Technik und Verkehr**	53
4.6.1	Datenschutzrechtliche Mängel bei Führerscheinstellen beanstandet	53
4.6.2	Was bei der Weitergabe von Führerscheinakten an medizinische Gutachter zu beachten ist	58
4.7	**Sozialwesen**	59
4.7.1	Überprüfungsbogen „Wohn- und Wirtschaftsgemeinschaft" revidiert	59
4.7.2	Angaben zur Sozialhilfe auf Überweisungsträgern	60
4.7.3	Sozialdatenschutz beim Publikumsverkehr	61
4.8	**Gesundheitswesen**	62
4.8.1	Chipkarten im Gesundheitswesen	62
4.8.2	Prüfung in einer psychiatrischen Klinik	65
4.8.3	Prüfung einer Suchtberatungsstelle	72
4.9	**Kultusbereich**	73
4.9.1	Aus dem Schulalltag	73
4.9.1.1	Der Umgang mit Entschuldigungsschreiben	73
4.9.1.2	Wenn Schüler „Mist bauen"	73
4.9.1.3	Verhaltensauffälligkeiten von Schülern	74
4.9.2	Videoaufzeichnungen für Unterrichtszwecke	75
4.9.3	Der gestohlene PC	76
5.	**Datenschutz bei den Gerichten**	76
5.1	Haftbefehle im Mülleimer	76
5.2	Prozeßkostenhilfeanträge nicht an die Gegenseite	77
6.	**Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung**	77
6.1	Datenschutzverordnung in Kraft getreten – Schleswig-Holstein setzt Maßstäbe	77
6.2	Ergebnisse von Prüfungsmaßnahmen im Bereich der automatisierten Datenverarbeitung	82
6.2.1	Beanstandungen akzeptiert – Abhilfe auf die lange Bank geschoben (2. Aufl.)	82
6.2.2	Kontrolle der Medizinischen Universität zu Lübeck abgeschlossen	84
6.2.3	Ein etwas anderes Prüfungsergebnis	87
6.2.4	Technische und organisatorische Anforderungen an ein „Ministeriumsrechenzentrum"	89
6.3	Mindestanforderungen an den Grundschutz für IT-Systeme	92
6.4	Sicherheitsvorkehrungen bei der Wartung von Computern	95

		Seite
7.	**Neue Medien und Technologien**	96
7.1	Telefonieren in Europa – Wirtschaftlichkeit vor Sicherheit?	96
7.2	Chipkarten – die nächste Computergeneration	98
8.	**Was es sonst noch zu berichten gibt**	101
8.1	Fehlerhafte Dateimeldungen binden Arbeitskraft	101
8.2	Virenprobleme offenbar größer als zugegeben	102
8.3	Vorschläge zur kostengünstigen Vernichtung von Altakten	102
8.4	Veröffentlichung behördlicher Telefonverzeichnisse als Postwurfsendung	103
8.5	Alle Eigentümer in einem Baugebiet sollten einander kennen – oder nicht?	103
8.6	Veröffentlichung von Prüfungsberichten der Rechnungsprüfungsämter	104
8.7	Verabschiedung eines Gleichstellungsgesetzes	104
8.8	Ermächtigung zur Sektenbeobachtung im Landesdatenschutzgesetz	104
8.9	Dokumentation von Übermittlungsersuchen der Verfassungsschutzbehörden an die Staatsanwaltschaft	105
8.10	Forschungsprojekt „Gläserne Schule"	105
9.	**Rückblick**	106
9.1	Protokollierung der Grundbucheinsicht realisiert	106
9.2	Verbesserung der Kapazitätsverordnung des juristischen Vorbereitungsdienstes	106
9.3	Neue Richtlinien sollen den Anspruch schwangerer Frauen auf anonyme Beratung sicherstellen	107
9.4	Übermittlung vollständiger Grundstückskaufverträge zur Ausübung des Vorkaufsrechts eingeschränkt	107
9.5	Akteneinsichtsrecht in Krankenakten der Psychiatrie durchgesetzt	108
9.6	Auskunftserteilung durch den Verfassungsschutz	108
10.	**DATENSCHUTZAKADEMIE**	109

1. Zur Situation des Datenschutzes in Schleswig-Holstein

1.1 Gesetzgebung, Kontrolle und Beratung

Schleswig-Holstein hat seine Gesetzgebung in den letzten Jahren in wesentlichen Teilen an die Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung angepaßt. Für die wichtigsten Verwaltungsbereiche liegen, flankiert durch das Landesdatenschutzgesetz, **bereichsspezifische Datenverarbeitungsbestimmungen** vor. Mit dem Erlaß der **Datenschutzverordnung** im vergangenen Jahr wurden Maßstäbe für eine sichere und ordnungsgemäße automatisierte Datenverarbeitung gesetzt (vgl. Tz. 6.1).

Nach wie vor ohne Rechtsgrundlage betreibt allerdings der Justizminister das landesweite Informationssystem für die Staatsanwaltschaften (GAST), in dem alle Personen gespeichert werden, gegen die ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist (vgl. Tz. 4.4.1). Der sog. „**Übergangsbonus**", auf den sich der Justizminister bislang immer berief, dürfte mit dem Ende der letzten Legislaturperiode des Deutschen Bundestages beim besten Willen **abgelaufen** sein. Mehrere Gelegenheiten, für eine verfassungskonforme Rechtsgrundlage zu sorgen, wie zuletzt die Verabschiedung des Verbrechensbekämpfungsgesetzes, blieben ungenutzt.

Das Land hat außer vielfältigen Interventionen in Bonn nichts Eigenständiges zuwege gebracht. Statt dessen wurde kurz vor Ablauf der Legislaturperiode ein Gesetzentwurf des Bundesrates unterstützt, der unter Datenschutzgesichtspunkten jeder Beschreibung spottet. Dadurch wurden die bis dahin vielleicht bestehenden Chancen des Landes gemindert, selbst gesetzgeberisch tätig zu werden. Wo immer der **Schwarze Peter** in dieser Frage letztlich hingeschoben wird, aus der Sicht der betroffenen Bürger wie sicherlich auch der Staatsanwälte, die täglich mit GAST arbeiten müssen, ist es ein **Skandal,** daß auch 14 Jahre nach Einführung des Systems noch keine gesetzliche Grundlage besteht. Ausgerechnet durch die Justiz selbst wird damit das **Volkszählungsurteil** des Bundesverfassungsgerichts **mißachtet**. Dabei dürfte gerade in Schleswig-Holstein in den vergangenen Monaten deutlich geworden sein, wie sensibel die Verarbeitung von Informationen darüber ist, wer gegen wen wann ein strafrechtliches Ermittlungsverfahren eingeleitet hat.

Der Schwerpunkt der Tätigkeit der Dienststelle hat sich im Berichtsjahr zur Kontrolle hin verlagert (vgl.Tzn. 4.1.1.1, 4.3.1, 4.3.6, 4.6.1, 4.8.2, 6.2). Neben erfreulichen Einzelbeispielen (vgl. Tz. 6.2.3) und einer **steigenden Aufgeschlossenheit** in den Behörden gegenüber den datenschutzrechtlichen Belangen der Bürger stellen wir immer wieder **Mängel bei der Umsetzung** des Datenschutzrechts und beim Umgang mit der automatisierten Datenverarbeitung fest.

Nach wie vor trennen sich viele Behörden nur ungern von einmal gesammelten Daten. So fanden wir bei Kontrollen in einer **psychiatrischen Klinik** die **Behandlungsakten** bis zu-

rück ins **letzte Jahrhundert** (vgl. Tz. 4.8.2). In einigen Führerscheinstellen haben wir festgestellt, daß **Strafurteile** und **Bußgeldbescheide** auch noch **Jahrzehnte** nach Löschung der entsprechenden Informationen im Bundes- und im Verkehrszentralregister gespeichert waren. Kommt dann noch der Umstand hinzu, daß inzwischen auch die Akten vernichtet wurden, bleibt nur die Hinweisspeicherung im Computer. Der Bürger kann dadurch leicht in die Rolle desjenigen geraten, der seine Unbescholtenheit erst beweisen muß, anstatt daß die Behörde den Beweis der Richtigkeit und Rechtmäßigkeit der Datenspeicherung antritt (vgl. Tz. 4.6.1).

Stichprobenkontrollen bei einzelnen **Kommunen** haben ergeben, daß nach wie vor Mängel bei der Umsetzung des Datenschutzrechts in die kommunale Praxis bestehen (vgl. Tz. 4.3.1).

Die Kontrollen im Bereich der **automatisierten Datenverarbeitung**, die auch im Berichtsjahr einen Schwerpunkt bildeten, zeigen, daß der sichere Umgang mit der Computertechnik für viele Behörden noch Zukunftsmusik ist. Der schnelle Ankauf von Technik und die Vereinfachung und Beschleunigung von Routineverfahren ist eine Sache; die Beherrschung der Technik unter Wahrung der für die Verwaltung geltenden Rechtsvorschriften eine andere, offenbar ungemein schwierigere.

So konnten wir feststellen, daß die Umsetzung der Verfahrensvorschriften für die automatisierte Datenverarbeitung zu wünschen übrig läßt (vgl. Tz. 6.2). Selbst in einem so sensiblen Bereich wie der **Verarbeitung medizinischer Daten** in einer Medizinischen Universität herrschten erhebliche Sicherheitsmängel (vgl. Tz. 6.2.2). Der ungestüme Aufbau der elektronischen Datenverarbeitung mit derzeit über 600, zum Teil miteinander vernetzten, PC stellte eine Universitätsklinik offenbar vor kaum lösbare Probleme. Noch nicht einmal das Geräteverzeichnis und die Dateibeschreibungen waren in Ordnung. Aber auch bei vermeintlichen Standardfragen wie der Nutzung von medizinischen Daten für Forschungszwecke stellten wir schwere Verstöße gegen die standesrechtlichen Bestimmungen fest.

Es gäbe also viel zu tun für den Datenschutz der Bürgerinnen und Bürger. Leider steht der **Datenschutz** in vielen Behörden trotz gestiegener Akzeptanz in der **Prioritätenskala** noch ziemlich weit **hinten**. Dabei mag man noch schmunzeln über die Aussage von Mitarbeitern einer geprüften Stelle, zur Datenlöschung kämen sie immer nur an den Tagen, an denen die Kollegen auf Betriebsausflug seien.

Wenn aber die Ergebnisse unserer Kontrollen akzeptiert, die notwendigen Konsequenzen jedoch **auf die lange Bank geschoben** werden, stellt sich für uns die Frage, ob es auf Dauer gutgehen kann, wenn der Ertrag teilweise aufwendiger Kontrollen letztlich durch ständiges Hintenanstellen in der Prioritätenskala zerredet wird (vgl. Tzn. 4.5.1, 6.2.1).

Neben der Kontrolle spielte auch die **Beratung** im Berichtsjahr wieder eine herausragende Rolle. Regionale Datenschutztage und DATENSCHUTZAKADEMIE haben dazu beigetragen, daß von den Behörden verstärkt der direkte Draht zur Dienststelle gesucht wird. Die Beratungsersuchen sind zahlreicher, aber auch detaillierter und spezifischer geworden. Viele Behörden haben erkannt, daß es für alle vorteilhafter ist, möglichst von vornherein Verstöße gegen das Datenschutzrecht zu vermeiden.

Die **Bürgereingaben** sind umfangreicher geworden und lassen erkennen, daß viele Betroffene über ihre Datenschutzrechte zumindest in den Grundzügen recht gut Bescheid wissen.

Deutlich zugenommen haben auch die **Beratungsersuchen** aus dem **politisch-parlamentarischen Raum**. Kaum ein Monat verging, in dem die Dienststelle nicht um Begutachtung einzelner Fragen, etwa der Offenbarungspflicht der Regierung gegenüber dem Parlament, gebeten wurde. Stets haben wir dabei versucht, zu Lösungen beizutragen, die sowohl dem Datenschutzrecht der Betroffenen als auch den Informationsrechten des Parlaments Rechnung trugen (vgl. Tz. 3.1).

Der weitere Ausbau des Kursangebots der DATENSCHUTZAKDEMIE (vgl. Tz. 10) ist ein Versuch, den Beratungsbedarf und die Vielzahl der Vortragswünsche, die an die Dienststelle herangetragen werden, zu bündeln und möglichst ökonomisch zu bewältigen.

1.2 Die personelle Ausstattung der Dienststelle

Die Zahl der Mitarbeiterinnen und Mitarbeiter – einschließlich Schreibdienst und Registratur – ist im Berichtsjahr auf 15 angewachsen. Für das Jahr 1995 hat der Landtag dankenswerterweise zwei **neue Stellen** des höheren Dienstes genehmigt. Mit ihrer Besetzung dürfte eine spürbare Intensivierung der Präsenz der Dienststelle in den Behörden eintreten. Damit hat das Parlament auch in Zeiten einer angespannten Haushaltslage ein deutliches Zeichen gesetzt.

Der technologische Wandel in der Informationsverarbeitung bedarf der begleitenden Kontrolle und Beratung zur Wahrung der Rechte der Bürgerinnen und Bürger. Deshalb müssen die **Aufwendungen für den Datenschutz** in einer angemessenen Relation zu den Kosten der Automatisierung der Datenverarbeitung stehen. Anläßlich der Beratung des 16. Tätigkeitsberichts im Parlament wurde dieser Zusammenhang erstmals deutlich herausgestellt. Unter anderem wurde die Frage erörtert, ob nicht die Beratungstätigkeit über Gebühreneinnahmen finanziert werden könnte. Auch wenn es gute Gründe geben mag, nicht so weit zu gehen, so hat doch das Parlament durch diese Debatte und nicht zuletzt durch die Verbesserung der Personalausstattung zu erkennen gegeben, daß ihm wohl bewußt ist, daß die Kosten für den Datenschutz die zwangsläufigen Folgen des Ausbaus der elektronischen Datenverarbeitung sind.

2. Der Weg in die Computergesellschaft

2.1 Neue Risiken für den Datenschutz der Bürgerinnen und der Bürger

Ein Fachmann führte kürzlich zum Tempo der technischen Entwicklung aus: „Bei den Personalcomputern ist es mittlerweile schon so weit, daß die Entwicklungszyklen schneller sind als der Druck der Kataloge, mit denen sie bestellt werden können." Selbst wenn er übertrieben hätte – wofür nichts spricht –, so macht das Beispiel deutlich, wie rasch sich die Computertechnik entwickelt.

Dieser **Trend** ist **ungebrochen.** Im vorliegenden Bericht wird in besonderer Weise auf die Chipkartentechnologie eingegangen (vgl. Tz. 7.2). Sie steht als nächste Computergeneration auf dem Weg der Miniaturisierung unmittelbar vor einer Explosion der Anwendungsgebiete.

Nachdem nun gerade erst auch in Schleswig-Holstein die **Krankenversicherungskarte** eingeführt wurde, wird diskutiert, ob nicht **weitere Karten** im Gesundheitswesen möglich wären. Zunächst auf freiwilliger Basis sollen hochsensible Daten zur Krankengeschichte, Behandlungsdaten, Blutgruppe, Gesundheitsrisiken etc. erfaßt werden. Bei Tests in unserem PC-Labor stellte sich schnell heraus, daß selbst die vergleichsweise harmlose Krankenversicherungskarte keineswegs fälschungssicher ist.

Es ist bezeichnend, daß bereits über Weiterentwicklungen nachgedacht wird, bevor überhaupt eine neue Technik erprobt und man in der Lage ist, sie sicher anwenden zu können (vgl.Tzn. 4.8.1 und 7.2). Nicht, daß die Chipkarte für das Recht auf informationelle Selbstbestimmung von vornherein negativ wäre. Eine Nutzung für mehr Freiheit und Freizügigkeit des einzelnen ist durchaus vorstellbar. Nur – wo bleibt die Zeit, um das Für und Wider sachlich und ruhig abzuwägen, wenn unter dem Diktat, Deutschland müsse in der Informationstechnologie führend sein, nur Hektik und kritiklose Übernahme des technisch Machbaren vorherrschen? Gewiß, die Prüfung der Argumente der Datenschutzbeauftragten und anderer zur **Sozialverträglichkeit** kann Zeit kosten; die Abwägung von Vor- und Nachteilen kann auch zum Ergebnis haben, ein neues Produkt sei nicht oder nicht so einzuführen. Wegen dieser Befürchtungen werden Sozialverträglichkeitsprüfungen leicht „vergessen" oder als unerwünschter Hemmschuh bezeichnet.

Während man in früheren Jahren damit rechnen konnte, daß neue Techniken erst nach Erprobung in der Wirtschaft mit zeitlicher Verzögerung – und damit häufig mit der Chance, Vor- und Nachteile gründlicher abzuwägen – in der öffentlichen Verwaltung zum Einsatz kam, fällt dieses **„Time-lag"** mehr und mehr weg. Der enorme Kostendruck, unter dem die öffentlichen Haushalte stehen und das daraus resultierende Bestreben, die öffentliche Verwaltung moderner und schlan-

ker zu machen, haben auch hier eine **Änderung der Bedingungen** bewirkt. Das Neueste und Modernste an Datenverarbeitungstechnik ist für die Behörden gerade gut genug. Schon wird darüber diskutiert, Chipkarten auch in der Verwaltung einzusetzen. Was zunächst bei den Asylbewerbern getestet werden soll (vgl. Tz. 4.1.3.4), könnte bald für alle in Serie gehen.

Die Begleitmusik, die der **Gesetzgeber** zu dieser technischen Entwicklung macht, ist alles andere als beruhigend. Immer offenkundiger wird, daß das Volkszählungsurteil des Bundesverfassungsgerichts nicht vollständig verstanden worden ist. Zwar wird auf vielen Gebieten versucht, die Datenverarbeitung mit wortreichen Vorschriften zu legalisieren. Die **vorrangige** kritische **Prüfung** der **Notwendigkeit** der einzelnen Maßnahmen wird aber entweder **unterlassen**, oder es wird vor den vollendeten Tatsachen kapituliert, die die Verwaltung längst geschaffen hat. So macht sich langsam Unbehagen darüber breit, daß sich vielleicht am Ende das Volkszählungsurteil nicht dahingehend ausgewirkt hätte, daß der Staat in weiser Selbstbeschränkung seine Datenverarbeitung auf ein unabdingbares Maß reduziert, sondern statt dessen dem in Jahrzehnten gewachsenen **Datenwust** nur ein **aufgeblähtes Paragraphenwerk** an die Seite gestellt hätte. Letztlich wäre der Grundsatz der Normenklarheit mit bloßer Detailgenauigkeit der Normen verwechselt worden.

Besonders markante Beispiele hierfür sind in der Ausländerverwaltung zu finden. Das **Ausländerzentralregistergesetz** legalisiert ein in Jahrzehnten gewachsenes Informationssystem über Ausländer, das für Deutsche seinesgleichen sucht (vgl. Tz. 4.1.3.3). Im Ausländerzentralregister werden Daten über Ausländerinnen und Ausländer zusammengeführt, die nicht zusammengehören. So als seien sie alle verdächtig, leicht straffällig zu werden, wird das Register rigoros für **sicherheitsbehördliche Belange** genutzt. Die **Geheimdienste** können mit seiner Hilfe ohne große rechtliche Hürden **Bewegungsprofile** über Ausländer anfertigen.

Nun sollen alle **Asylbewerber** auch noch zwangsweise mit einer **Chipkarte** ausgerüstet werden, auf der ihre Daten gespeichert sind. Für jeden, der ein entsprechendes Lesegerät besitzt, wären die Asylbewerber dann gläsern. Gewiß werden eine Menge „guter Gründe" anzuführen sein, etwa daß es gelte, dem Asylmißbrauch entgegenzuwirken, die unberechtigte Inanspruchnahme staatlicher Leistungen zu verhindern, ja daß es doch letztlich im Interesse der Asylbewerber selbst liege, daß bei den Ämtern alles möglichst glatt und reibungslos läuft. Wer bei solcher Argumentation beifällig nickt, mag bedenken, daß eine Datenverarbeitung, die heute nur Ausländer oder Asylbewerber betrifft, schon morgen Markenzeichen einer „modernen" Verwaltung allgemein werden könnte.

2.2 Modernisierung der Verwaltung

Die öffentliche Finanznot hat im Bund und in den Ländern eine breite Diskussion über die „Modernisierung" der öffentlichen Verwaltung hervorgebracht. In Schleswig-Holstein legten im Berichtsjahr die **„Projektgruppe Modernisierung des öffentlichen Sektors"** der Ministerpräsidentin einen Statusbericht und die **„Enquete-Kommission zur Verbesserung der Effizienz der öffentlichen Verwaltung"** des Landtages ihren Schlußbericht vor. Beide Dokumente enthalten eine Fülle von Ideen, Vorschlägen und Modellprojekten, mit denen die öffentliche Verwaltung effizienter gemacht werden soll. Einige davon haben auch unmittelbaren Bezug zum Recht auf informationelle Selbstbestimmung.

2.2.1 Verzicht auf Datenfriedhöfe

So ist immer die Rede davon, die **Verwaltung** solle **schlanker** werden. Der Begriff beinhaltet sicher viele Facetten, unter anderem auch den Verzicht auf überflüssige Informationen. Im Schlußbericht der Enquete-Kommission werden überkommene Berichtspflichten kritisiert, die beim Empfänger zu keiner anderen Reaktion als zum Abheften und damit dem Anlegen von **Datenfriedhöfen** führten. Dies ist eine Feststellung, die auch wir bei unseren Kontrollen immer wieder treffen müssen. Auch in diesem Bericht gibt es davon einige Kostproben (vgl. Tzn. 4.5.2, 4.6.1). Zumeist wird uns zur Begründung entgegengehalten: „Das haben wir immer so gemacht".

Die moderne Computertechnik mit ihren immensen Speicherkapazitäten verführt geradezu zu übermäßigen Datensammlungen. Dabei wird in der Regel verkannt, daß das bequeme Abspeichern von Daten auf **billigen Massenspeichern** eine Sache ist; der Aufwand für die Pflege und die spätere sinnvolle Nutzung der Daten werden häufig nicht gesehen.

Zum Bild der schlanken Verwaltung gehört deshalb auch die **Beschränkung** auf das **absolut notwendige Minimum** an personenbezogenen Daten. Eben nicht nur um des informationellen Selbstbestimmungsrechts der Betroffenen willen, sondern weil eine schlanke Verwaltung unnötigen Datenballast nicht verträgt oder mit anderen Worten: Der schlanke Staat braucht auch eine **schlanke Datenverarbeitung.**

2.2.2 Bedingungen für den Computereinsatz

In allen Reformüberlegungen für die öffentliche Verwaltung spielt der **verstärkte Einsatz** der **Computertechnik** eine herausragende Rolle. Ohne Zweifel lassen sich durch eine Automatisierung der Informationsverarbeitung an vielen Stellen Rationalisierungsgewinne erzielen. Hinzu kommt, daß gerade junge Mitarbeiter der öffentlichen Verwaltung den Computer gewissermaßen als Standardausrüstung ihres Arbeitsplatzes erwarten.

Wer konventionelle Datenverarbeitungsverfahren durch automatisierte ersetzt, muß aber eine Reihe von Gesichtspunkten bedenken, die das farbenfrohe Bild der schnellen Rationalisierung möglicherweise etwas trüben. Die meisten IT-Systeme sind für den Gebrauch in der Wirtschaft oder anwendungsneutral konstruiert. Sie bedürfen sozusagen **geeigneter Adapter**, wenn sie in der öffentlichen Verwaltung eingesetzt werden sollen. Dies ist beileibe nicht nur technisch gemeint, sondern schließt die notwendigen organisatorischen, verfahrensmäßigen und vor allem auch auf die Qualifizierung der Mitarbeiter und der Führungsebene zielenden Begleitmaßnahmen ein. Wer sich unvorbereitet in die **Abhängigkeit** von **Computern** begibt, kann ein böses Erwachen erleben.

Deshalb ist es im Ansatz richtig und bedarf der konsequenten Beachtung, wenn der **Finanzminister** in einem **Runderlaß** jüngst erneut darauf hingewiesen hat, daß Haushaltsmittel für neue IT-Vorhaben nur veranschlagt werden dürfen, wenn die einschlägigen Planungs- und Verfahrensregelungen eingehalten sind. In diesem Zusammenhang muß auch rechtzeitig geprüft werden, ob die rechtlichen Voraussetzungen für das Verfahren erfüllt sind, damit peinliche Zwangslagen wie bei GAST (vgl. Tzn. 1.1, 4.4.1) gar nicht erst entstehen. Auch die Voraussetzungen für einen sicheren und ordnungsgemäßen Verarbeitungsprozeß müssen gegeben sein, bevor er in Gang gesetzt wird.

2.2.3 Realistische Kostenrechnung

Eng mit dem Vorstehenden hängt ein weiterer zentraler Reformansatz zusammen. Das überkommene Haushaltsrecht wird als ungeeignet für eine nach wirtschaftlichen Grundsätzen arbeitende Verwaltung angesehen. Deshalb sollen **neue Steuerungsmodelle** erprobt werden. Zu ihnen gehören auch **transparente Kostenrechnungen**, aus denen sich die tatsächlichen Verursacher bestimmter Ausgaben erkennen lassen. Zu Recht geht die Enquete-Kommission in ihrem Schlußbericht davon aus, daß mit dem wachsenden Einsatz der Informationstechnik gesteigerte Anforderungen an Datenschutz und Datensicherung entstehen (S. 63). Noch knapper formuliert die kommunale Gemeinschaftsstelle (KGSt) in ihrem Bericht 2/1994 (S. 7): „Wer technikunterstützte Informationsverarbeitung will, muß auch Datenschutz sagen".

Es würde die Bemühungen um mehr Kostenehrlichkeit ad absurdum führen, würde man die **Kosten für Datenschutz und Datensicherheit** nicht von Anfang an angemessen einkalkulieren. Es gehört auch zur **Kostenehrlichkeit**, sich darüber im klaren zu sein, daß mit der zunehmenden Automatisierung der Datenverarbeitung auch **zunehmender Kontrollaufwand** verbunden ist. Was an der einen Stelle eingespart wird, muß an anderer Stelle zumindest teilweise wieder für Schulungsmaßnahmen zur internen Datenschutzkontrolle und zur angemessenen Anpassung der Personalausstattung

beim Landesbeauftragten für den Datenschutz an die technische Entwicklung ausgegeben werden. Nicht die Einzelposition, sondern die **Gesamtrechnung** ist also **entscheidend**.

2.2.4 Privatisierung verwässert den Datenschutz

Die Privatisierung von Tätigkeitsfeldern der Verwaltung wird als ein wichtiges Mittel zur „Verschlankung" betrachtet. Bei näherem Hinsehen weisen die Überlegungen beträchtliche Differenzierungen auf. Es geht von der vollständigen Verlagerung einer Aufgabe auf die Privatwirtschaft über die „formale" Privatisierung bis hin zur Auftragsvergabe im Einzelfall.

Für den Datenschutz der betroffenen Bürger haben die jeweiligen Maßnahmen unterschiedliche Konsequenzen. Jede Form der **Privatisierung**, die zum Ergebnis hat, daß statt des Landesdatenschutzgesetzes und anderer bereichsspezifischer Verarbeitungsvorschriften das Datenschutzrecht für den Privatbereich anwendbar wird, führt in der Tendenz zu einer **Schlechterstellung** der **Bürger** und der **betroffenen Mitarbeiter** in ihren **Datenschutzrechten**. Denn an die Stelle von zumeist präzisen und am Grundsatz der Erforderlichkeit orientierten Vorschriften treten dann die bequemen **Generalklauseln** des **Bundesdatenschutzgesetzes**, die in vielen Punkten die datenverarbeitende Stelle gegenüber dem Bürger bevorzugen.

Der **Bundesgesetzgeber** bleibt deshalb gerade im Hinblick auf die Privatisierungsbestrebungen in der öffentlichen Verwaltung nachdrücklich aufgefordert, endlich den Datenschutz im Privatbereich zu verbessern, die Generalklauseln durch bereichsspezifische Vorschriften zu ergänzen und insgesamt für ein **gleichwertiges Schutzniveau** im öffentlichen wie im privaten Bereich zu sorgen.

Bei der bestehenden Rechtslage ist deshalb aus der Sicht des Datenschutzes denjenigen Modellen der Aufgabenauslagerung der Vorzug zu geben, bei denen die öffentliche Hand **Verantwortung** und **Kontrolle** über den Datenverarbeitungsprozeß behält. Hierfür stellt das Landesdatenschutzgesetz in der Gestalt der Vorschriften über die **Auftragsdatenverarbeitung** die geeigneten rechtlichen Instrumente zur Verfügung (vgl. Tz. 4.2.1).

2.2.5 Abbau obrigkeitsstaatlicher Strukturen

Die Reformvorschläge thematisieren den Abbau obrigkeitsstaatlicher Strukturen unter zwei Gesichtspunkten: Zum einen **offenes, transparentes Verhalten** gegenüber dem Bürger. An die Stelle obrigkeitsstaatlicher Attitüde sollen **Dialog** und **Konsensualprinzip** treten. Diese Überlegung trifft im Bereich der Verarbeitung personenbezogener Daten auf ein wohlvorbereitetes Feld. Auch die **Datenschutzgesetze** gehen mit ihren **Instrumenten der Transparenz** wie Normenklarheit, Aufklärung bei der Datenerhebung und Auskunftsanspruch des Bürgers von einem Bild der öffentlichen Verwaltung aus,

mit dem sich Wissensvorsprung und Geheimnistuerei als Machtinstrumente der Behörden gegen den Bürger nicht vertragen. Deshalb wäre es zu begrüßen, wenn diese Möglichkeiten auch von Bürgern und Verwaltung souverän genutzt würden und ihre bisherige Beschränkung auf die Speicherung personenbezogener Daten durch Gewährleistung **allgemeiner Informationsansprüche** überwunden würde.

Der zweite Aspekt, der in der Reformdiskussion häufig angesprochen wird, ist die Veränderung **interner Verwaltungsstrukturen**. An die Stelle von Bevormundung und Weisung von oben sollen dezentrale **Eigenverantwortlichkeit** und **Motivation** treten. Auch insoweit fühlen wir uns mit unserer Doppelstrategie bestätigt, die Beratung und Kontrolle gleichermaßen als Mittel zur Motivation der Behörden einsetzt, sich den Datenschutz der Bürger zur eigenen Angelegenheit zu machen.

2.2.6 Verfassungsrechtliche Grenzen

Aus den **Grundrechten** und dem Rechtsstaatsprinzip ergeben sich **Grenzen** für die Veränderung der Verwaltungsabläufe. So muß ein **Verwaltungsverfahren** trotz Vereinfachung und (Teil-) Automatisierung **rechtsstaatlichen Grundsätzen** entsprechen. Das Verwaltungshandeln muß, auch wenn es in automatisierter Form erfolgt, **nachvollziehbar** und **kontrollierbar** sein. **Effektiver Rechtsschutz** muß auch möglich sein, wenn das Verwaltungsverfahren nur noch auf Computerdisketten dokumentiert ist. **Materielle Gerechtigkeit** im Einzelfall muß auch angestrebt werden, wenn Computerprogramme für formale Gleichbehandlung sorgen.

Auch aus dem Recht auf informationelle Selbstbestimmung ergeben sich Folgerungen für den Modernisierungsprozeß, die rechtzeitig bedacht sein wollen. Die **Datenverarbeitung** muß für den Bürger, soweit er von ihr betroffen ist, **transparent** bleiben, auch wenn sie immer komplexer und leistungsfähiger wird. Die **Zweckbindung** der Daten setzt der Möglichkeit der Mehrfachnutzung von Daten und dem bequemen Online-Abruf zwischen verschiedenen speichernden Stellen Grenzen. Das verfassungsmäßige **Verbot automatisierter Persönlichkeitsprofile** steht der Zusammenführung von Daten aus den unterschiedlichsten Lebensbereichen, z.B. mit Hilfe eines einheitlichen **Personenkennzeichens** oder von Chipkarten, entgegen, auch wenn dies im Sinne einer am Markt orientierten Rationalisierung noch so wünschenswert erschiene.

Schon diese wenigen Aspekte, die keineswegs abschließend aufgezählt sind, zeigen, daß die öffentliche Verwaltung die Arbeitsprinzipien der privaten Wirtschaft nicht ungeprüft übernehmen darf. Was bei letzterer im Interesse eines möglichst hohen Gewinnes angemessen sein mag, muß für den Bereich der Verwaltung kritisch hinterfragt werden. Der **„Gewinn" der Verwaltung** ist nicht aus Bilanzen und Überschüssen abzulesen, sondern besteht auch darin, daß die Bürger sich

auf ein rechtsstaatliches, faires Verfahren verlassen können, das ihre Grundrechte respektiert.

3. Datenschutz im Parlament

3.1 Befugnisse parlamentarischer Untersuchungsausschüsse im Lichte des Datenschutzes

Die Tätigkeit des „Schubladenausschusses" wirft Fragen nach dem Verhältnis seiner Ermittlungsrechte zum Datenschutzrecht auf. Über die Zulässigkeit von Beweisanträgen muß jeweils im konkreten Fall entschieden werden.

Nachdem wir uns bereits 1993 generell zum Umfang des Beweiserhebungsrechts eines parlamentarischen Untersuchungsausschusses geäußert hatten (16. TB, S. 31 f.), wurden wir auch im Berichtsjahr um Stellungnahmen zur Zulässigkeit einzelner Beweisbeschlüsse gebeten. Insbesondere Auskünfte über **finanzielle Transaktionen** auf den **Privatkonten** von Bürgern, die vom Untersuchungsausschuß teilweise pauschal und für verhältnismäßig lange Zeitabschnitte erbeten wurden, haben wieder die Frage nach dem **Umfang des Aufklärungsanspruchs** eines Parlaments in den Vordergrund treten lassen.

Dem verfassungsmäßigen Recht des einzelnen auf Datenschutz steht **gleichrangig** der verfassungsrechtliche Anspruch des Untersuchungsausschusses auf Information gegenüber. Die notwendige **Rechtsgüterabwägung** ist bei **jedem Beweisbeschluß** von neuem zu treffen. Dabei muß der Ausschuß Entscheidungen treffen, durch die das Beweiserhebungsrecht und der grundrechtliche Datenschutz einander so zugeordnet werden, daß beide soweit wie möglich ihre Wirkungen entfalten (Flick-Urteil des Bundesverfassungsgerichts). Zudem sollte das Parlament Vorkehrungen für den Geheimschutz treffen.

Diese abstrakt formulierten Grundsätze bereiten in der Praxis deshalb besondere Schwierigkeiten, weil Untersuchungsgegenstand des „Schubladenausschusses" gerade der Verdacht ist, daß Maßnahmen aus dem Verantwortungsbereich von Regierung und Parteien sowie privates Engagement miteinander verflochten waren. Deshalb müssen gerade private Aktivitäten daraufhin überprüft werden, in welcher Beziehung sie zu den amtlichen stehen. Dazu kann es auch gehören, **auffällige private Kontenbewegungen** zu bewerten.

Allerdings ließen einige der Beweisbeschlüsse Zweifel aufkommen, ob sie zu dem Beweisthema noch in einem angemessenen Verhältnis stehen. Dies war vor allem der Fall, als pauschal alle Kontenbewegungen für mehrere Jahrgänge erhoben werden sollten. Hier hätte durch eine möglichst enge **zeitliche Eingrenzung** erfragter Kontenbewegungen sowie durch eine Spezifizierung der interessierenden Transaktionen (z.B. auf Buchungen von mehr als einer bestimmten Summe oder durch eine Beschränkung auf regelmäßig wiederkehren-

de Leistungen) Rücksicht auf Betroffene genommen werden sollen.

Wie sehr allerdings die Meinungen über die Zulässigkeit entsprechender Auskunftsersuchen auseinandergehen können, wird aus den **Reaktionen** der vom Ausschuß angesprochenen **Banken** deutlich. Sie reichen von Ablehnung über den Versuch, eine Eingrenzung der erbetenen Daten zu erreichen, bis hin zu unkritischen Vollauskünften. Offenbar bestehen bei diesen Stellen unterschiedliche Auffassungen sowohl hinsichtlich des parlamentarischen Informationsanspruchs als auch hinsichtlich der Bedeutung vertraglicher Bindungen zwischen Bank und Kunden.

Der datenschutzrechtliche Inhalt solcher Verträge – und damit der Umfang des „Bankgeheimnisses" – ist nach unserer Auffassung im BDSG nur unzulänglich geregelt und führt gerade an der Schnittstelle zwischen privaten und öffentlichen Interessen immer wieder zu Unsicherheiten.

Grundsätzliche Überlegungen sind auch bei der Frage anzustellen, welche **staatsanwaltschaftlichen Unterlagen** über den verstorbenen Ministerpräsidenten **Dr. Barschel** im Untersuchungsausschuß vorzulegen sind. Nach der Landesverfassung kann eine solche Vorlage abgelehnt werden, „wenn schutzwürdige Interessen einzelner, insbesondere des Datenschutzes, entgegenstehen". Datenschutzrechtliche Maßstäbe sind zwar nur bei Informationen über natürliche, also lebende Personen, nicht aber über Verstorbene anzulegen; jedoch gilt nach der Rechtsprechung des Bundesverfassungsgerichts (sog. „Mephisto-Beschluß") der grundrechtliche Schutz der Menschenwürde über den Tod hinaus.

Im Regelfall entscheidet und verantwortet die Exekutive die Herausgabe der Unterlagen allein. Dies kann aber speziell im Verhältnis zu den Informationsansprüchen eines parlamentarischen Untersuchungsausschusses nicht uneingeschränkt gelten. Hier empfiehlt sich die **Beteiligung des Ausschusses** (z.B. der Vorsitzenden oder der Obleute) an der Vorauswahl der zur Verfügung zu stellenden Unterlagen (vgl. Flick-Urteil des Bundesverfassungsgerichts).

Eine kritische Prüfung jedes einzelnen Beweisantrages anhand dieser Kriterien ist auch in der weiteren Arbeit des Parlamentarischen Untersuchungsausschusses angezeigt.

3.2 Beantwortung parlamentarischer Anfragen durch die Landesregierung

Nach der Landesverfassung kann die Landesregierung die Beantwortung von Fragen aus dem Landtag ablehnen, wenn schutzwürdige Interessen einzelner entgegenstehen. Wann dies zulässig ist, entscheidet sich an den Umständen des Einzelfalls.

Immer häufiger werden wir bei Zweifelsfragen über den Umfang der Auskunfts- und Aktenvorlagepflicht der Regierung

gegenüber dem Parlament um Rat gefragt, so auch bei der **Großen Anfrage** der CDU-Fraktion zur **Personalpolitik** der Landesregierung an den Landesbeauftragten mit der Bitte um datenschutzrechtliche Stellungnahme herangetragen.

Deren Inhalt war von der Fragestellung her zunächst datenschutzrechtlich neutral. Es wurde nämlich nicht nach Informationen über einzelne natürliche Personen gefragt. Aus bestimmten Kombinationen konnten sich jedoch sehr kleine Fallzahlen ergeben, die dann mit geringen **Zusatzinformationen** (z.B. Geschäftsverteilungspläne, Telefonverzeichnisse) zum **Personenbezug** der Daten führen konnten.

Wir haben deshalb empfohlen, wegen des weit verbreiteten Zusatzwissens über personelle Gegebenheiten in der Landesverwaltung von Detailinformationen im Rahmen der Großen Anfrage dann abzusehen, wenn weniger als fünf Fälle gleiche Merkmalsausprägungen hatten.

Als unproblematisch können nur solche personenbezogenen Angaben angesehen werden, deren Inhalt offenkundig bekannt ist. Das trifft z.B. auf aktuelle Einstufungen von Mitarbeitern zu, die in Geschäftsverteilungsplänen festgehalten sind oder, wie bei Beförderungen, einem größeren Personenkreis bekannt werden. Es kann generell davon ausgegangen werden, daß **Laufbahninformationen** aus der Zeit nach Einstellung in den Landesdienst für Betroffene keinem besonderen Vertrauensschutz unterliegen. Das gleiche gilt, wenn die Betroffenen mit einer Weitergabe von Daten einverstanden waren, z.B. wenn ihre Einstellung zu Pressemitteilungen und Darstellungen ihrer Laufbahn in der Öffentlichkeit geführt hat.

3.3 Datenschutzregelung für das Parlament

Das Landesdatenschutzgesetz gilt nicht für die inneren Angelegenheiten des Parlaments. Es will sich deshalb seine eigene Datenschutzordnung geben. Der Entwurf sollte noch verbessert werden.

Wir haben uns bereits (16. TB, S. 16) dazu geäußert, wie der praktische Umgang der Landtagsverwaltung mit den personenbezogenen Daten der Abgeordneten gestaltet werden sollte. Daneben wurde schon vor einiger Zeit im Parlament die Notwendigkeit erkannt, auch für die **Parlamentsarbeit** selbst zusammenfassende Grundvorschriften über den Datenschutz zu schaffen. Denn das LDSG ist dort nicht unmittelbar anwendbar und kann nur als Auslegungshilfe bei Einzelfragen herangezogen werden. Wir sind gebeten worden, zu den Entwürfen Stellung zu nehmen.

Es ist beabsichtigt, in einer **parlamentarischen Datenschutzordnung** vergleichbare Grundsätze des Datenschutzes für das Parlament vorzusehen, wie sie die Datenschutzgesetze für die Exekutive festlegen. In weitem Umfang soll durch Verweisungen der materielle Gehalt der Datenschutzgesetze übernommen werden.

Der Anwendungsbereich der Datenschutzordnung soll sich auf „parlamentarische Aufgaben" beziehen, und die Datenverarbeitung soll insgesamt nur für **„parlamentarische Zwecke"** zulässig sein. Weiter sollen die Abgeordneten zur Verschwiegenheit verpflichtet werden. Schließlich soll auf die Datenschutzordnung nur dann zurückgegriffen werden, wenn nicht andere Vorschriften, wie etwa das Abgeordnetengesetz oder das Untersuchungsausschußgesetz, speziellere Regelungen enthalten.

Wir haben die Überlegungen des Landtages begrüßt und darauf hingewiesen, daß das Datenschutzrecht des Parlaments möglichst so wie das allgemeine Datenschutzrecht gestaltet sein sollte, sofern nicht die andersartige Aufgabe und Arbeitsweise des Parlaments etwas anderes gebieten.

Wichtig wird es jedoch sein, **„parlamentarische Aufgaben"** konkreter von solchen Aktivitäten der Abgeordneten **abzugrenzen**, die sich zwar im politischen, aber nicht im parlamentarischen Bereich, z.B. in Verbänden, Parteien o.ä., vollziehen. Je exakter dies bereits in der Datenschutzordnung definiert ist, um so weniger wird eine künftige Praxis mit Abgrenzungsschwierigkeiten zu kämpfen haben.

Bedenken haben wir allerdings dagegen geäußert, daß **alle parlamentarischen Aktivitäten** als ein **einheitlicher Zweck** angesehen werden sollen, an den die Datenverarbeitung gebunden wäre. Das würde bedeuten, daß Daten innerhalb des gesamten parlamentarischen Raumes ohne Einhaltung irgendwelcher Zweckbindungen verwendet werden dürften. Hier sollte nach unserer Auffassung geprüft werden, ob nicht **Differenzierungen** in den Aufgabenbereichen eines Parlaments berücksichtigt werden müssen. Die Datenverarbeitung bei der Haushaltskontrolle folgt anderen Anforderungen als bei Gesetzgebungsvorhaben. Eingaben an den **Petitionsausschuß** sind anders zu behandeln als Mitteilungen aus anderen Bürgerkontakten, Gesundheits- und Steuerdaten anders als personenbezogene Informationen aus Pressemeldungen. In jedem Fall sollte bei solchen personenbezogenen Informationen, die Betroffene freiwillig für einen bestimmten Zweck zur Verfügung stellen, ausschließlich diese Zweckbestimmung für die weitere Verarbeitung der Daten zugrunde gelegt werden.

Der Erlaß einer Datenschutzordnung würde nicht nur eine Klärung datenverarbeitungsrechtlicher Verhältnisse im Landtag selbst bringen, sondern auch auf die **Zusammenarbeit** von **Legislative** und **Exekutive** ausstrahlen und Bedeutung für die Auskunftspflicht der Landesregierung gegenüber dem Landtag haben. Die Wirksamkeit einer solchen Datenschutzordnung wäre nämlich bei der Prüfung der Schutzwürdigkeit von Einzelinteressen im Zusammenhang mit Auskünften der Landesregierung zu berücksichtigen. Dies könnte dazu führen, daß die Landesregierung eher zu Auskünften und zur Herausgabe von Unterlagen bereit sein müßte.

4. Datenschutz in der Verwaltung

4.1 Allgemeine und innere Verwaltung

4.1.1 Personalwesen

4.1.1.1 Erste Beanstandungen wegen Verletzung des neuen Personalaktenrechts

Die gesetzlichen Vorgaben für das Personalaktenrecht sind auf eine neue Grundlage gestellt worden. Der praktische Umgang mit den Daten folgt jedoch weitgehend der alten Gewohnheit.

Der Umgang mit den Personaldaten der Beamten ist seit dem 01.01.1993 im **Beamtenrechtsrahmengesetz** präzise geregelt. Die vorgeschriebene Anpassung des Landesbeamtengesetzes befindet sich in Vorbereitung. Für **Angestellte** und **Arbeiter** sind die neuen Rechte **entsprechend anzuwenden**.

Bei der Umsetzung des neuen Rechts gibt es in der Praxis offensichtlich nicht unerhebliche Probleme und Defizite, was sich in Anfragen und Beschwerden niederschlägt.

- Bei einer Stadt wurde eine Stelle nach einer internen Auslese neu besetzt. Den unterlegenen Bewerbern aus dem eigenen Haus wurden die für ihre Person entscheidenden **Faktoren** für die **Nichtberücksichtigung** mitgeteilt. Allerdings wurden die entsprechenden Schreiben den Betroffenen **„auf dem Dienstweg"**, also über die zuständigen Fachamtsleiter, zugeleitet. Dieser Personenkreis verfügt über kein eigenes Zugangsrecht zu Personalakten. Die Bekanntgabe der Gründe verletzte deshalb die Vertraulichkeit der Personalakten.
- Zwischen einem Mitarbeiter und seinem Fachamtsleiter war es zu einem Streit über die stellenplanmäßige Ausweisung seiner Planstelle sowie über die Zuordnung von Aufgaben durch den Geschäftsverteilungsplan gekommen. Die Stellungnahmen der Beteiligten, die für den Mitarbeiter nicht günstig waren, **heftete** das Personalamt in dessen **Personalakte**, obwohl sein **Dienstverhältnis** in keiner Weise berührt war. Da die Unterlagen keine „Personalaktendaten", sondern Organisationsfragen enthalten, durften sie nicht in die Personalakte aufgenommen und mußten folglich entfernt werden.
- Einer Behörde war angezeigt worden, ein Beamter verstoße gegen das Nebentätigkeitsrecht. Nach umfangreichen Ermittlungen stellte sich dies schließlich als unzutreffend heraus. Der Vorgang betraf zunächst zweifelsfrei das Grundverhältnis des Beamten und war deshalb zu seiner Personalakte zu nehmen. Das Beamtenrechtsrahmengesetz schreibt jedoch vor, daß **Behauptungen**, falls sie sich als **unbegründet** oder **falsch** erwiesen haben, mit Zustimmung der Beamtin oder des Beamten unverzüglich aus der **Personalakte** zu entfernen und zu vernichten sind. Auf unsere Beanstandung hin wurde entsprechend verfahren.

– Eine Beamtin hatte schriftlich darum gebeten, ihr die Gründe für die Abrundung einer bewilligten Beihilfe zu nennen. Auf dem Schreiben der Betroffenen wurden vom Personalamt folgende handschriftliche Vermerke angebracht: „Der Laie staunt ..." sowie „Wer den Pfennig nicht ehrt...". Die auf dem Dokument enthaltenen **unsachlichen Vermerke** waren zur rechtmäßigen Aufgabenerfüllung des Dienstherrn nicht erforderlich. Sie waren, weil kein unmittelbarer innerer Zusammenhang dieses Dokuments zum Dienstverhältnis der Betroffenen festgestellt werden konnte, aus der Personalakte zu entfernen.

4.1.1.2 Wohin mit Arbeitszeitkarten?

Arbeitszeitkarten sind materieller Bestandteil der Personalakte und gehören in die Personalabteilung. Fachvorgesetzte können mit der Arbeitszeitkontrolle beauftragt werden.

Die Neuregelung der Personaldatenverarbeitung im Beamtenrecht wirkt sich auch auf den Umgang mit **Arbeitszeitdaten** aus. Durch das neue Recht sind alle Unterlagen unter besonderen Schutz gestellt worden, die mit dem Dienstverhältnis eines Beamten in einem unmittelbaren inneren Zusammenhang stehen (**Personalaktendaten**). Entsprechende Dokumente sind materieller Bestandteil der Personalakte.

Die **Arbeitszeitkontrolle** steht mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang. Die hierzu geführten Unterlagen gehören deshalb für die Dauer ihrer Speicherung zur Personalakte (ggf. Teilakte) und unterliegen hinsichtlich des Zugriffs den o.a. Beschränkungen.

Ist Fachvorgesetzten auch die **Dienstaufsicht** über ihre Mitarbeiter übertragen worden, benötigen sie auch Arbeitszeitdaten. Diese können ihnen deshalb z.B. zu Vorkontrollen, Abgleichen mit Dienstkalendern u.ä. zur Kenntnis gegeben werden.

4.1.1.3 Vergleichsmitteilungen zur Berechnung des Ortszuschlages überflüssig?

Für Vergleichsmitteilungen zur Berechnung des Ortszuschlages gibt es derzeit keine Rechtsgrundlage. Es bestehen auch Zweifel, ob derartige Mitteilungen überhaupt notwendig sind.

Nach dem Bundesbesoldungsgesetz wird bei verheirateten Mitarbeitern der im **Ortszuschlag** enthaltene Sozialzuschlag gekürzt, wenn beide im öffentlichen Dienst beschäftigt sind. Gleiches gilt für Beschäftigte bei privaten Stellen, wenn die Vergütungsstruktur der des öffentlichen Dienstes entspricht. In solchen Fällen der Anspruchskonkurrenz sollen nach den geltenden Verwaltungsvorschriften zum Bundesbesoldungsgesetz unverzüglich **Vergleichsmitteilungen** zwischen den

beteiligten Arbeitgebern ausgetauscht werden. In einem konkreten Fall war auf dieser Grundlage die Eheschließung einer Landesbeamtin einem privaten Arbeitgeber mitgeteilt worden, obwohl der Ehegatte an seinem Arbeitsplatz über die Heirat aus persönlichen Gründen zunächst Stillschweigen bewahren wollte.

Das Landesdatenschutzgesetz läßt eine Datenverarbeitung nur zu, wenn entweder die Betroffenen eingewilligt haben oder dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt. Diese Voraussetzungen waren hier nicht erfüllt, da **Verwaltungsvorschriften** wegen fehlender Rechtsnormqualität **nicht Befugnisgrundlage** für Datenübermittlungen sein können. Zudem schreibt das Beamtenrechtsrahmengesetz für Auskünfte über Personalaktendaten an Dritte grundsätzlich die Einwilligung des Betroffenen vor.

Die geprüfte Stelle hat in Abstimmung mit dem Finanzminister des Landes zugesagt, die Versendung von Vergleichsmitteilungen ohne Einwilligung der Betroffenen künftig zu unterlassen. **Vergleichsmitteilungen** dürften ohnehin in den meisten Fällen **überflüssig** sein, da jeder Arbeitgeber für sich die Anspruchsvoraussetzungen für die Zahlung eines Sozialzuschlages zu prüfen hat. Der **Betroffene** hat dazu ggf. entsprechende **Nachweise** über die Besoldung bzw. Vergütung seines Ehegatten vorzulegen. Eine Notwendigkeit für zusätzliche Kontrollmaßnahmen ist in diesem Zusammenhang nicht zu erkennen.

4.1.1.4 Intime Informationen über Verwandte in Beihilfeanträgen – eine Chance wurde nicht genutzt

Wer Beihilfe für seine Angehörigen beantragt, kann aus den Arztrechnungen vertrauliche medizinische Daten entnehmen. Vor allem bei getrennt lebenden Ehepaaren stößt dies häufig auf Bedenken. Bei der bestehenden Rechtslage ist aber Abhilfe kaum möglich.

Mitarbeiter der öffentlichen Verwaltung erhalten Beihilfen zu Krankheitskosten. Mit ihren Anträgen und den **eingereichten Unterlagen** geben sie ihrem Dienstherrn Informationen über eigene Krankheiten und über solche berücksichtigungsfähiger **Angehöriger**. In Eingaben wurde das Problem aufgeworfen, ob bei einem derartigen Verfahrensablauf der Beihilfeberechtigte nicht ohne Not in die Lage versetzt werde, sich über **persönliche Tabubereiche** seiner Angehörigen zu unterrichten. Es wurden etwa HIV-Untersuchungen, gynäkologische Beratungen bei Schwangerschaftsabbrüchen und Krankheitsdaten getrennt lebender Ehegatten oder volljähriger Kinder genannt, die von besonderer Sensibilität sind.

Das Problem ist, daß derzeit nur der Mitarbeiter selbst beihilfeberechtigt ist. Angehörige haben keine eigenen Ansprüche und müssen daher der Beihilfestelle die Grundlagen für Beihilfezahlungen immer **über den Antrag des Berechtigten**

mitteilen. Deshalb kann die Tatsache ärztlicher Beratung, die Art der Krankheit und die Höhe der Kosten nur dann vertraulich gehalten werden, wenn der beihilfeberechtigte Mitarbeiter damit einverstanden ist und etwa durch Antragsformulare mit Blankounterschrift oder durch Bezugnahme auf getrennt eingereichte Unterlagen selbst auf eine Kenntnisnahme verzichtet. Das **Einverständnis** des Beihilfeberechtigten lag aber gerade in den Problemfällen, die in den Eingaben geschildert waren, nicht vor.

Eine bessere Lösung böte ein **eigener Beihilfeanspruch** für **Familienangehörige**, der nach unserer Auffassung nicht grundsätzlich mit dem Dienstrecht oder gar den hergebrachten Grundsätzen des Berufsbeamtentums unvereinbar wäre. Entsprechende Änderungen der Beihilfevorschriften waren aber in zurückliegenden Bund-Länder-Beratungen und bei der Neugestaltung des Personalaktenrechts **nicht durchsetzbar**. Diskretion kann in diesem Bereich also bei der gegenwärtigen Rechtslage nur dann gewahrt werden, wenn alle Beteiligten dazu bereit sind. Angehörige könnten sich sonst regelrecht gezwungen sehen, auf Beihilfeleistungen zu verzichten, wollen sie Informationen über ärztliche Kontakte für sich behalten.

4.1.1.5 Verarbeitung von Bewerberdaten im Rahmen von internen Personalausleseverfahren

Ein unterlegener Bewerber hat nach der Rechtsprechung des OVG Schleswig-Holstein Anspruch auf Information über die Gründe der Bewerberauswahl.

Bei der datenschutzrechtlichen Prüfung von Personalausleseverfahren standen im Berichtsjahr meist Fragen nach der **Erforderlichkeit einzelner Bewerberdaten** im Vordergrund. Das Landesbeamtengesetz stellt dazu fest, daß die Auswahl der Bewerber nach Eignung, Befähigung und fachlicher Leistung ohne Rücksicht auf Geschlecht, Abstammung, Rasse, Glauben, religiöse oder politische Anschauung, Herkunft oder Beziehungen zu erfolgen hat. Entsprechende Verfahren müssen demnach auf der Grundlage **objektiver** und **nachprüfbarer Kriterien** durchgeführt werden.

Das **Schleswig-Holsteinische Oberverwaltungsgericht** hatte die Frage zu entscheiden, ob und in welchem Umfang für Bewerber im Rahmen einer **internen Stellenbesetzung** ein Informationsanspruch ggf. auch über Daten der Mitbewerber besteht. Das Gericht hat dazu ausgeführt (B.v. 16.04.93, 3 M 15/93), daß Mitbewerber einen Anspruch darauf haben, **vor** der **Beförderung** eines Kollegen über Auswahl und Verfahren **informiert** zu werden, um dann eine Rechtsverletzung prüfen und ggf. gegen die Auswahlentscheidung vorgehen zu können.

Weiter heißt es in dem Beschluß: „Zum **Informationsanspruch** gehört, daß dem abgelehnten Bewerber neben dem Ergebnis auch mitgeteilt wird, welche entscheidenden **Wer-**

tungsfaktoren der Dienstherr zugrunde gelegt hat. Es muß deutlich werden, ob dem erfolgreichen Bewerber aus qualifikationsbezogenen Erwägungen oder unter Zugrundelegung eines oder mehrerer Hilfskriterien der Vorrang eingeräumt worden ist. Wenn dem abgewiesenen Bewerber nur der Name des ausgewählten Bewerbers mitgeteilt wird, kann er nicht effektiv prüfen, ob sein Anspruch auf rechtsfehlerfreie Bescheidung seines Gesuchs unter Beachtung des Leistungsprinzips verletzt wurde".

Wir halten diesen **Informationsanspruch** auch unter datenschutzrechtlichen Gesichtspunkten für **vertretbar**. Der Schutz des Persönlichkeitsrechts findet seine Grenzen, soweit dabei in Rechte Dritter eingegriffen wird. Dies ist bei der Bewerberauslese durchweg der Fall. In einer solchen Konkurrenzsituation muß ein Bewerber – jedenfalls soweit es zur Rechtswahrnehmung durch den Konkurrenten erforderlich ist – hinnehmen, daß auch ihn betreffende Personaldaten im Rahmen des Auswahlverfahrens an seine Konkurrenten übermittelt werden.

4.1.2 Öffentliche Sicherheit

4.1.2.1 Immer neue Befugnisse für die Polizei – wo bleibt die Sicherheitsdividende?

In den letzten Jahren sind der Polizei immer neue Möglichkeiten eröffnet worden, bei der Verfolgung von Straftaten Daten zu erheben und zu verarbeiten. Vor der Überprüfung, ob hierdurch bessere Erfolge in der Kriminalitätsbekämpfung erreicht wurden, will die Polizei sich offenbar drücken.

Neue Verbrechensformen erfordern neue Aufklärungskonzepte – zweifellos. Warum aber müssen sich diese hauptsächlich darauf konzentrieren, die ohnehin gefährdete **Privatsphäre** des Bürgers noch weiter zu beschränken? Dies sei für eine wirksame Bekämpfung und vorbeugende Verhinderung von Straftaten insbesondere im Bereich der Rauschgift- und organisierten Kriminalität nun einmal unumgänglich, wird argumentiert. In den letzten Jahren sind Schritt für Schritt **neue gesetzliche Eingriffsbefugnisse** beschlossen worden, z.B. für

- den Einsatz verdeckter Ermittler,
- den erweiterten Einsatz technischer Mittel (Abhörgeräte, Videokameras, Peilsender usw.),
- die Verpflichtung der Banken zur Meldung größerer Bargeldtransaktionen,
- die Übermittlung von Erkenntnissen der Geheimdienste an die Polizei,
- den gezielten Einsatz des Bundesnachrichtendienstes bei der Überwachung drahtloser Fernmeldeverbindungen,
- die Rasterfahndung.

Angesichts der Schwere dieser neuen Eingriffsbefugnisse sollte man entsprechende Erfolgsmeldungen bei der Aufklärung erwarten dürfen. Die Innenminister der Länder haben auf Drängen der Datenschutzbeauftragten bereits vor einiger Zeit beschlossen, im Rahmen einer kritischen **Erfolgskontrolle** zu überprüfen, ob die neu gewährten Eingriffsbefugnisse den gewünschten Erfolg gezeigt haben.

Da die versprochenen Bilanzen auf sich warten ließen, haben wir beim **Innenminister** nachgefragt. Außer der Betonung, bei diesen Befugnissen handele es sich um „unverzichtbare Instrumente zur Verbrechensbekämpfung" haben wir jedoch zu unserem Erstaunen zunächst erfahren, daß der durch den Einsatz dieser Mittel erzielte Erfolg nicht meßbar bzw. nicht kontrollierbar sei. Zur Begründung wurde u.a. angeführt, einheitliche Kriterien, nach denen sich ein Erfolg beurteilen ließe, existierten nicht.

Nunmehr haben die Innenminister beschlossen, zu überlegen, wie man den „Erfolg" näher definieren könne und welche Kriterien hierzu aufzustellen seien. Diese nicht besonders schnelle Gangart spiegelt die Schwierigkeiten der Sicherheitsbehörden wieder, über Erfolge **Rechenschaft** ablegen zu müssen. Dies ist sicherlich zunächst mit Arbeit verbunden und mit dem Zwang, sich über Maßstäbe und Verfahren einigen zu müssen. Aber wäre die Wahrung unserer Grundrechte dies nicht wert?

Doch genau hier „liegt der Hase im Pfeffer". Zwar wollen das Bundeskriminalamt (BKA) sowie einige Länder eine **„Rechtstatsachensammelstelle"** gründen, von der die entsprechende Arbeit geleistet werden könnte. Doch träfe die Arbeitsbelastung, die durch das Auswerten nach einem Erhebungsraster und die Anlieferung entstünde, weitgehend die Länder. Aus Beschlußempfehlungen der vorbereitenden Projektgruppe aus dem vergangenen Jahr wird deutlich, daß dies, aber auch ganz andere Motive wohl dazu führen werden, daß die Rechtstatsachen mit einer bestimmten Zielrichtung ausgewertet werden sollen. Es heißt dort u.a. wörtlich:

„Vorschlag:
Auf eine systematische Erhebung des Erfolges ... wird verzichtet.

Begründung:

Die mangelnde Konkretisierbarkeit des Erfolges bei Maßnahmen der genannten Art könnte unter bestimmten Bedingungen auch zu rechtspolitisch unerwünschten Konsequenzen führen (so könnten beispielsweise fehlende „Erfolge" bei Telefonüberwachungsmaßnahmen (TÜ) dazu führen, die TÜ hinsichtlich bestimmter Katalogtatbestände als solche in Frage zu stellen). Darüber hinaus würde die anlaßbezogene Überprüfung der genannten besonderen polizeilichen Ermittlungsmaßnahmen auf konkrete, unmittelbar auf sie zu stützende Erfolge hin, zu einem erheblichen Arbeitsaufwand besonders in den Ländern führen, der außer Verhältnis zum Erfolg stün-

de. **Die Projektgruppe empfiehlt daher, auf diese Position im Erhebungsraster zu verzichten.**"

Derselbe Vorschlag, nämlich kein repräsentatives Material auf Bundesebene zu sammeln, wird aus ähnlichen Gründen auch hinsichtlich der anderen Eingriffsermächtigungen gemacht. Die traurige Quintessenz des ganzen ist also, daß man sich derzeit auf **keine tatsächliche Erfolgskontrolle** und damit wohl auch nicht auf die Einrichtung einer zentralen Sammelstelle auf Bundesebene einigen kann.

Die Initiatoren wollen jedoch auf das argumentativ wertvolle Instrument einer zentralen „Fallsammlung" nicht verzichten. Sie haben nämlich erkannt, daß die Bürger nicht mehr bereit sind, immer neue und immer weiterreichende Eingriffe in ihre Privatsphäre widerspruchslos hinzunehmen. Um dennoch auch in Zukunft **Forderungen** nach **weiteren Eingriffsbefugnissen** stellen zu können, soll jetzt eine „Bund/Länder-Fallsammlung" eingerichtet und dort nur noch gezielt entsprechendes Material gesammelt werden.

So heißt es in den Berichten der Projektgruppe weiter:

„Auf eine systematische Erhebung und Mitteilung der sich bei Durchführung der unter I. 1 bis 4 aufgeführten Maßnahmen ergebenden tatsächlichen und rechtlichen Schwierigkeiten wird verzichtet. Die Meldungen sollten sich daher auf die anlaßbezogene Darstellung echter Problemfälle beschränken, mit denen entsprechende rechtspolitische Forderungen gestellt und untermauert werden können."

Damit ist die Katze aus dem Sack. Wer bisher noch nicht so recht verstanden hat bzw. es nicht glauben mag, in welchem Ausmaß hier zum Zwecke der **Beeinflussung der öffentlichen Meinung** einseitig Material gesammelt werden soll, dem wird es durch die Vorschlagsbegründungen in beiden Berichten nochmals verdeutlicht. Dort heißt es wörtlich:

„Die Informationserhebung sollte sich dabei an folgendem Raster orientieren:

- Darstellung der Schwachstellen (z.B. Fehlen von Rechtsgrundlagen für polizeiliche Eingriffe, Schwierigkeiten bei der Durchführung polizeilicher Maßnahmen oder der Anwendung rechtlicher Vorschriften)
- Beschreibung des Bedarfs (etwa nach Beibehaltung bisheriger Regelungen, nach Ergänzung bestehender bzw. Schaffung neuer gesetzlicher Bestimmungen)
- Begründung des Bedarfs
- Darstellung der Konsequenzen einer Nichtregelung
- Vorschläge für die rechtspolitische Umsetzung
- Darstellung spektakulärer Erfolgsfälle zur Bestätigung rechtspolitischer Auffassungen

Die Erhebung und Darstellung sollte umfassend sein und sich auf wenige echte (gewichtige) Problemfälle zum zweifels-

freien Aufzeigen der Grenzen polizeilicher Möglichkeiten beziehen."

Demnach müssen wir also befürchten, künftig auf der Basis von einigen wenigen, jedoch **plakativen Einzelfällen** mit „rechtspolitischen Reforminitiativen" konfrontiert zu werden. Dies ergibt sich auch aus der abschließenden Begründung für den Vorschlag der Projektgruppe, eine Bund/Länder-Fallsammlung einzurichten:

„Rechtspolitische Forderungen aus der polizeilichen Praxis sind mit gewichtigen eindeutigen Fallbeispielen zu belegen. Die Erfahrung zeigt, daß ohne derartige Rechtstatsachen Bedürfnisse z.B. nach Einführung neuer gesetzlicher Ermächtigungen strafprozessualer Art oder der Ergänzung/Verbesserung von gesetzlichen Straftatbeständen politisch praktisch nicht durchsetzbar sind. Wird kein einschlägiges Fallmaterial präsentiert, besteht deshalb schon von seiten der verantwortlichen Ressorts auf Ministeriumsebene i.d.R. auch keine Bereitschaft, rechtliche Verbesserungsvorschläge aufzugreifen und umzusetzen.

Der Einrichtung einer Bund/Länder-Fallsammlung – die es bisher für diesen Bereich nicht gibt – bei der Rechtstatsachensammelstelle kommt daher eine außerordentlich große Bedeutung zu. Bei voller Akzeptanz in Bund und Ländern und funktionierendem Meldedienst kann sie zu einem respektablen Unterstützungsinstrument für diejenigen Stellen/Gremien werden, die für das Aufgreifen und Umsetzen von rechtspolitisch erheblichen Verbesserungsvorschlägen aus dem Polizeibereich zuständig sind."

Es zeigt sich hier überdeutlich, daß manche Sicherheitsbehörden einmal erhaltene Befugnisse hüten wie einen kostbaren Schatz und sich mit allen Mitteln dagegen sträuben, sie einer ehrlichen (Selbst-)Prüfung zu unterziehen. Erfreulicherweise teilt der Innenminister meine Bedenken gegen die Vorgehensweise der Projektgruppe. Er hat den Beschlußvorschlag des Bundeskriminalamtes abgelehnt, weil auch nach seiner Auffassung die dort verwendete Argumentation den Verdacht erweckt, als sei man an einer objektiven Darstellung nicht interessiert. Wir werden den Innenminister bei seinem Bemühen unterstützen, in den Gremien der Innenministerkonferenz auf eine sachgerechte Behandlung des Themas hinzuwirken.

4.1.2.2 Europol

Europol soll für weite Kriminalitätsbereiche zuständig sein. Die Definition der von den Datensammlungen Betroffenen ist vage. Die ausschließliche Verantwortung der erhebenden Stelle für die Weiterverarbeitung der Daten ist nicht sichergestellt.

Die Notwendigkeit einer polizeilichen Zusammenarbeit über Staatsgrenzen hinweg ist in den letzten Jahren viel diskutiert und auf europäischer Ebene bis hin zu entsprechenden Ver-

tragsentwürfen konkretisiert worden. Unter der Bezeichnung **„Europol"** soll eine supranationale Polizeibehörde entstehen, die auch über eigene Datenbestände verfügen wird. Die Unterzeichnerstaaten beabsichtigen, Europol alle personenbezogenen Informationen zur Verfügung zu stellen, von denen sie annehmen, daß sie auch für die anderen Polizeibehörden von Interesse sein könnten.

Während der erste Vertragsentwurf sich noch vergleichsweise akzeptabel darstellte (es sollten nur die Daten von Personen an Europol übermittelt werden, von denen angenommen wird, daß sie im Bereich des internationalen Rauschgifthandels und der organisierten Kriminalität tätig sind), ist der **Bereich der strafbaren Handlungen**, mit denen sich Europol beschäftigen soll, in den nachfolgenden Entwürfen **drastisch ausgeweitet** worden. Nach dem letzten Stand wird Europol „zunächst" bei der **Verhütung und Bekämpfung**

- des illegalen Drogenhandels,
- der Nuklearkriminalität,
- des illegalen Handels mit Waffen, Munition und Sprengstoffen,
- des illegalen Technologietransfers,
- des Menschenhandels und der illegalen Einschleusung,
- der Ausbeutung der Prostitution,
- des Raubes und der Erpressung (insbesondere Schutzgelderpressung),
- der Umweltkriminalität,
- der Kraftfahrzeugkriminalität (insbesondere Verschiebung in andere Staaten sowie Diebstahl von Transportgütern),
- des illegalen Handels mit Kunstgegenständen und Antiquitäten (insbesondere im Zusammenhang mit Einbruch, Diebstahl und Hehlerei) sowie
- der mit diesen Kriminalitätsformen verbundenen illegalen Geldwäschehandlungen

tätig. Eine Erweiterung dieser Bereiche ist jederzeit durch einstimmigen Ratsbeschluß möglich.

Gespeichert werden sollen zudem nicht nur personenbezogene Informationen über **Täter** oder **Tatverdächtige**, sondern auch Daten von

- Personen, die bei einer **künftigen Strafverfolgung** als **Zeugen** in Betracht kommen,
- Personen, bei denen Anhaltspunkte bestehen, daß sie **Opfer** einer **künftigen Straftat** werden können,
- **Kontakt-** und **Begleitpersonen** sowie
- **Hinweisgebern** und **sonstigen Auskunftspersonen**.

Datenschutzrechtlich ist insbesondere die Speicherung von Informationen zu den beiden letztgenannten Personenkreisen zu kritisieren. Sie sind so **vage umschrieben**, daß bereits

jeder Betroffene, der aus Sicht der Polizei irgendwo im Umfeld eines Verdächtigen auftaucht, europaweit gespeichert werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich auch einhellig dagegen, daß Europol diese Daten **in eigener Zuständigkeit** verwalten soll. Bisher ist in der Bundesrepublik jedes Bundesland für die von ihm in länderübergreifende Systeme eingegespeicherten Daten selbst verantwortlich. Schnitte man nunmehr z.B. die Möglichkeit ab, einmal an Europol übermittelte Daten umgehend wieder zu löschen, wenn die Verdachtsmomente hinfällig geworden sind, so würde dies die Verantwortungen verwischen und die Rechte der Betroffenen entscheidend einschränken.

Hinzu kommt, daß nach den bisherigen Plänen **Rechtsschutz** gegen eine unberechtigte Datenverarbeitung nur beim Europäischen Gerichtshof in Luxemburg und nicht bei den deutschen Gerichten möglich sein soll. Darüber hinaus könnte Europol selbständig entscheiden, ob und in welchen Fällen Daten an andere Polizeibehörden der Mitgliedsländer übermittelt werden. Bei dem zu erwartenden Umfang des Informationsaustausches wäre es den Bürgern dann so gut wie unmöglich zu erkennen, wo überall Daten über sie gespeichert sind.

Wenn, wie geplant, die Befugnis geschaffen wird, Informationen auch an Geheimdienste weiterzugeben, ist die Gefahr, daß ein **europaweiter undurchschaubarer Datendschungel** entsteht, nicht von der Hand zu weisen.

4.1.2.3 KpS-Richtlinien in Kraft

In den vergangenen Jahren ist versucht worden, eine Präzisierung der Regelungen zu erreichen, nach denen die Polizei personenbezogene Daten speichern darf. Nunmehr sind die „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien)" in Kraft gesetzt worden.

Die neuen Richtlinien regeln eine Reihe bisher noch offen gebliebener Punkte aus den in den vergangenen Jahren durchgeführten Kontrollen der polizeilichen Datenverarbeitung:

- Definiert werden erstmalig die Zwecke, zu denen Datensammlungen angelegt werden sollen.
- Für jede Aktensammlung, die diesen Zwecken dienen soll, ist eine **Errichtungsanordnung** vorgeschrieben, die entweder vom Leiter des Landeskriminalamtes oder vom jeweiligen Behördenleiter getroffen werden muß. Damit ist ausgeschlossen, daß einzelne Kommissariate oder Sachbearbeiter nach Belieben personenbezogene Informationen über Betroffene in „besonderen Dateien" speichern.
- Der Zusammenhang zwischen dem **Ausgang des Ermittlungsverfahrens** und der **Speicherungsdauer** wird näher festgelegt. Die aktenführende Dienststelle wird verpflich-

tet, sich nach dem Ausgang des Ermittlungsverfahrens zu **erkundigen**. soweit dieser noch nicht bekannt ist. Wird das Verfahren durch die Justiz nicht innerhalb von zwei Jahren abgeschlossen, so ist jährlich zu prüfen, ob die Daten noch benötigt werden. Ist der Tatverdacht entfallen, sind die dazugehörigen Unterlagen auszusondern.

- Ein **Negativkatalog** legt fest, daß keine personenbezogenen Unterlagen angelegt werden dürfen bei:
  - Kleinkriminalität von Erwachsenen,
  - Ermittlungsverfahren, bei denen die Richtlinien zur Förderung der Diversion bei jugendlichen und heranwachsenden Beschuldigten zur Anwendung gelangten,
  - Taten von Kindern, die das 12. Lebensjahr noch nicht vollendet haben, es sei denn, daß sie unter Anleitung oder Duldung strafrechtlich verantwortlicher Personen an den Taten beteiligt gewesen sind,
  - Verkehrsdelikten, es sei denn, daß sich aus speziellen Gründen ein Anlaß zur Speicherung ergibt,
  - Ordnungswidrigkeiten.

Wesentlich vereinfacht wird der Umgang mit **Auskunftsanträgen Betroffener**. Für deren Bearbeitung ist zentral das Landeskriminalamt zuständig, das anhand der polizeilichen Erkenntnisdatei die entsprechenden Akten zusammenzieht und dem Antragsteller so eine umfassende Auskunft geben kann.

Insgesamt kann man mit den neuen Richtlinien, an deren Erarbeitung wir mitgewirkt haben, unter datenschutzrechtlichen Gesichtspunkten zufrieden sein. Sie können einen Beitrag zu mehr Rechtssicherheit und damit auch zu größerer Offenheit zwischen Bürger und Polizei leisten.

4.1.2.4 Mangelhafte Kontrollierbarkeit von PED-Abfragen

Für eine wirksame datenschutzrechtliche Kontrolle hat sich die bisherige Aufbewahrungsfrist der Protokolldaten über Abfragen der PED (Polizeiliche Erkenntnisdatei) als zu kurz erwiesen.

Immer wieder wenden sich Petenten an uns mit dem Verdacht, über sie seien rechtswidrig Informationen aus der PED abgerufen und verbreitet worden. So meldete sich z.B. ein Kommunalpolitiker, nachdem ihn sein Kontrahent mit Kenntnissen konfrontiert hatte, die seiner Ansicht nach nur aus den polizeilichen Dateien stammen konnten. Im Prinzip können derartige Zweifelsfragen durch **Auswertung der Protokolle**, die über jede Abfrage der PED aufgezeichnet werden, geklärt werden. Die Protokolldaten werden jedoch bereits **nach 50 Tagen vernichtet**.

In den von uns zu überprüfenden Fällen hat diese **kurze Frist** oft zur Folge gehabt, daß nicht geklärt werden konnte, ob zu den Personalien des Petenten Daten aus dem Polizeisystem abgerufen worden waren. Betroffene werden mit Informationen, von denen sie annehmen müssen, daß sie aus dem polizeilichen Datenverarbeitungssystem stammen, häufig geraume Zeit nach einer eventuell erfolgten Abfrage konfrontiert. Manchmal ergeben sich Anhaltspunkte für eine möglicherweise rechtswidrige Recherche nur durch Zufall, so daß gar kein bestimmter Zeitpunkt genannt werden kann. Aus diesen Gründen haben wir uns dafür eingesetzt, die Aufbewahrungsfrist für die Protokolldaten auf sechs Monate auszudehnen. Dabei gehen wir davon aus, daß es auch im Interesse der Polizei liegt, möglichst alle auftretenden Zweifelsfälle klären zu können.

4.1.2.5 COMPAS

Die EDV-Unterstützung bei der Bearbeitung von Massensachen in den Polizeirevieren wird vom Innenminister weiter vorangetrieben. Bislang liegt uns jedoch noch kein schriftliches verbindliches Konzept vor.

Bereits im letzten Tätigkeitsbericht (16. TB, S. 30) hatten wir über dieses derzeit größte Automatisierungsvorhaben des Innenministers berichtet. Die von uns für eine einzelne Pilotinstallation aufgestellten Forderungen wurden zwar weitgehend erfüllt. Eine abschließende datenschutzrechtliche Beurteilung und Beratung ist derzeit jedoch noch nicht möglich, da der Innenminister bisher **kein einheitliches Konzept** mit verbindlichen, schriftlichen Soll-Vorgaben vorgelegt hat. Dies wird u.a. damit begründet, daß im Verlaufe der Projektierung und insbesondere Programmierung der einzelnen Verfahrensschritte so viele Änderungen gegenüber ursprünglichen Vorstellungen notwendig seien, daß eine vorherige Festschreibung keinen Sinn ergebe. Eine schriftliche Verfahrensdokumentation werde fast zeitgleich mit dem Programm fertiggestellt und stimme dann auch mit diesem überein. Änderungen, insbesondere auch datenschutzrechtliche Änderungswünsche, könnten dann immer noch eingearbeitet werden.

Diese Vorgehensweise weicht von der herkömmlichen in starkem Maße ab und **erschwert** die abschließende **datenschutzrechtliche Beurteilung** eines derartigen Projektes erheblich. Hier wird insbesondere darauf zu achten sein, daß keine Fakten geschaffen und spätere Änderungserfordernisse mit dem Hinweis auf erhebliche Kosten zurückgewiesen werden.

4.1.3 Ausländerverwaltung

4.1.3.1 Kein Zwang zur Selbstbezichtigung für Asylbewerber

Das Grundrecht auf Asyl erfordert eine faire und sachgerechte Verfahrensgestaltung. Die von Asylbewerbern vorgetragenen Verfolgungsgründe dürfen grundsätzlich nicht

gegen sie zum Zwecke der Strafverfolgung verwendet werden.

Im Zuge der Begründung seines Asylantrages hatte ein Asylbewerber vor dem Verwaltungsgericht auch über politische Aktivitäten außerhalb seines ihm zugewiesenen Aufenthaltsortes berichtet, da er glaubte, nur auf diese Weise sein Asylbegehren schlüssig vortragen zu können. Der entsprechende Schriftsatz an das Gericht war in Durchschrift auch der zuständigen Ausländerbehörde als Verfahrensbeteiligter zugeleitet worden. Diese unterrichtete daraufhin die Staatsanwaltschaft, um ein **Strafverfahren** wegen **Verletzung** der **Aufenthaltsbestimmung** gegen den Asylbewerber einzuleiten. Dieser beschwerte sich gegen die nach seiner Auffassung unzulässige Datenübermittlung.

Aus dem strafprozessualen und auch **verfassungsrechtlich** verankerten **Grundsatz**, daß niemand gezwungen werden darf, sich selbst einer Straftat zu bezichtigen und damit zu seiner Überführung beizutragen, hat das **Bundesverfassungsgericht** (BVerfG) ein strafprozessuales Verwertungsverbot für die Fälle abgeleitet, in denen Betroffene aufgrund bestehender Auskunftspflichten in anderen Verfahren zur Offenbarung eigener Straftaten gezwungen sind. Die Voraussetzungen für ein solches **Verwertungsverbot** liegen nach unserer Auffassung in dem dargestellten Fall vor.

Der **Bundesgerichtshof (BGH)** hat zwar in einem vermeintlich ähnlichen Fall, in dem es um die Darlegung der rechtswidrigen Modalitäten der Einreise eines Asylbewerbers ging, festgestellt, daß dessen Mitwirkungspflicht nach dem Asylverfahrensgesetz schließlich nicht mit Sanktionen belegt sei und eine Aussageverweigerung deshalb nur zu einem erhöhten Beweisrisiko führe, welches nicht die Annahme eines Verwertungsverbots rechtfertige. Er ließ jedoch gleichzeitig die Frage unbeantwortet, ob etwas anderes gilt, wenn dem Betroffenen gewichtige oder gar existentielle Nachteile drohen. Eine andere Sichtweise ist nach Auffassung des Gerichts z.B. dann geboten, wenn die Verweigerung der Angaben stets und zwangsläufig zur Folge hat, daß der Antragsteller seinen Anspruch auf Anerkennung des Asylrechts nicht verwirklichen kann.

Der entscheidende Unterschied zu dem hier zu beurteilenden Fall bestand aber gerade darin, daß die Darlegung der Einreisemodalitäten tatsächlich nur geringen Einfluß auf den Ausgang des Asylverfahrens hatte. Für den Petenten, der sich an uns gewandt hatte, mußte es in seinem Verfahren jedoch darauf ankommen, möglichst **alle entscheidungserheblichen Fakten** zur Beurteilung der Gefahr politischer Verfolgung **vorzutragen**. Werden von Asylbewerbern bei der heutigen Entscheidungspraxis nicht alle Möglichkeiten zur schlüssigen Darstellung der Verfolgungsgefahr genutzt, riskieren sie die Ablehnung ihres Asylantrags.

Zudem berücksichtigt das Urteil des BGH nicht ausreichend die maßgebliche Verfassungslage. Das BVerfG hat in einem Beschluß ausdrücklich dargelegt, daß „von der gefestigten

Rechtsprechung des BVerfG auszugehen ist, nach der **Grundrechtschutz** weitgehend auch durch die **Gestaltung des Verfahrens** zu bewirken ist, und daß die Grundrechte demgemäß nicht nur das gesamte materielle, sondern ebenso das Verfahrensrecht beeinflussen, soweit dieses für einen effektiven Grundrechtsschutz von Bedeutung ist. Da die wirksame Durchsetzung der materiellen Asylrechtsverbürgung eine dafür geeignete Verfahrensregelung voraussetzt, ist auch hier das Verfahrensrecht von verfassungsrechtlicher Relevanz." An dieser Auffassung hat das BVerfG seitdem festgehalten.

Demgemäß muß die Gestaltung des **Asylverfahrens** sachgerecht auf eine möglichst **effektive Grundrechtswahrnehmung** gerichtet sein. Bei der Ausgestaltung der Verfahrensgrundsätze muß folglich die Situation des Asylbewerbers berücksichtigt werden, der unter Umständen beim Verlassen Deutschlands schwerwiegende und nicht korrigierbare Folgen hinnehmen muß. Er hat deshalb ein schützenswertes Interesse, im Asylverfahren seine politische Verfolgung auch unter vollständiger Darlegung der entscheidungserheblichen Sachverhalte nachweisen zu können. Wegen dieser weitreichenden Folgen gebietet das Grundrecht auf Asyl gerade solche verfahrensrechtlichen Vorkehrungen, die der Gefahr unanfechtbarer Fehlurteile entgegenwirken.

Eine Beschränkung der Möglichkeit, im Rahmen der Anhörung **alle entscheidungserheblichen Sachverhalte** vorzutragen, ohne sich gleichzeitig einer strafrechtlichen Verfolgung auszusetzen, würde demnach grundsätzlich Art. 16 a Grundgesetz widersprechen. Schranken dürften allenfalls dann bestehen, wenn im Einzelfall das öffentliche Interesse an einer Strafverfolgung, etwa wenn es sich um besonders schwerwiegende Straftaten handelt, gegenüber der Gewährleistung des Grundrechts auf Asyl überwiegt.

Nach alledem hielten wir ein Verwertungsverbot für die in dem Asylverfahren durch eigene Angaben des Betroffenen bekannt gewordenen Umstände einer strafbaren Handlung für gegeben. Auch wiederholte **Verstöße** gegen **Aufenthaltsbeschränkungen** sind nur als verhältnismäßig **geringfügige Straftat** zu werten. Bei einmaligem Verstoß erfolgt nur eine Ahndung als Ordnungswidrigkeit. Wir haben uns gegenüber der betroffenen Kreisverwaltung deshalb auf den Standpunkt gestellt, daß die Angaben des Asylbewerbers nicht gegen ihn selbst verwendet werden dürfen.

4.1.3.2 Übermittlung von Asylbewerberdaten an die Telekom

Meldebehörden dürfen den Aufenthaltsstatus von Ausländern nicht an die Telekom übermitteln.

Ein **Ausländer** hatte bei der Telekom einen Antrag auf Einrichtung eines **Fernsprechanschlusses** gestellt. Statt des gewünschten Telefons erhielt er jedoch zunächst die Aufforderung, eine **Sicherheitsleistung** von 1.000 DM zu erbringen,

weil bei Asylbewerbern grundsätzlich „die Gefahr von Entgeltsausfällen" drohe. Auf Nachfrage erfuhr der Betroffene, daß die Telekom generell bei Personen mit ausländischem Namen versucht, deren Aufenthaltsstatus bei der zuständigen Wohnsitzgemeinde zu ermitteln. Im konkreten Fall hatte die betroffene **Amtsverwaltung** tatsächlich eine entsprechende **Auskunft** erteilt.

Für derartige Datenübermittlungen ist weder im Landesmeldegesetz noch im Asylverfahrensgesetz eine Rechtsgrundlage enthalten. Das Verhalten der Meldebehörde war damit als **Verstoß** gegen geltendes **Datenschutzrecht** zu beanstanden.

4.1.3.3 Ausländerzentralregister – nach dem Gesetz nun die Verordnung

Das Ausländerzentralregistergesetz erweitert die Funktionen des Registers über das Maß dessen hinaus, was gegenüber deutschen Staatsangehörigen als verfassungsrechtlich vertretbar angesehen würde. Der Entwurf einer Durchführungsverordnung konkretisiert diese Nutzungsmöglichkeiten nicht in der datenschutzrechtlich gebotenen restriktiven Weise.

Bereits im 14. Tätigkeitsbericht (14. TB, S. 31 f.) haben wir die Vorstellungen zu einem Ausländerzentralregistergesetz kritisiert und dabei auf die Gefahren hingewiesen, die mit einem umfangreichen **multifunktionalen Online-Auskunftssystem** verbunden sind. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat datenschutzrechtliche Bedenken gegen das Gesetz erhoben. Es ist dennoch praktisch unverändert verabschiedet worden. Dadurch wird das Ausländerzentralregister u.a. als umfassendes Melde-, Fahndungs-, Personenstands- und Aktensuchsystem gesetzlich festgeschrieben, während die vergleichbaren Funktionen für deutsche Staatsangehörige von unterschiedlichen, zum Teil länderspezifischen, Registern erfüllt und durch vielfältige spezialgesetzliche Vorschriften geregelt werden.

In unserer **Stellungnahme** zum Entwurf der **Durchführungsverordnung** haben wir vorgeschlagen, die zu weit formulierten Vorschriften des Gesetzes einzuschränken und zu detaillieren.

Dies sollte insbesondere

- durch Stärkung der Mitverantwortung der Stellen, die dem Register Daten übermitteln,
- durch strenge Zulassungsvoraussetzungen für die Einrichtung automatisierter Abrufverfahren und
- durch Einschränkung der Voraussetzungen für sogenannte Gruppenauskünfte, die praktisch einer Art Rasterfahndung gleichkommen

geschehen.

So sollten z.B.

- im Register nur **bestandskräftige Entscheidungen** in Ausländerangelegenheiten gespeichert werden oder zumindest auf die Vorläufigkeit solcher Entscheidungen hingewiesen werden; anderenfalls besteht die Gefahr erheblicher Fehlinterpretationen zu Lasten der Betroffenen;
- **Berichtigungen** nur mit Beteiligung der für die ursprünglich erhobenen Daten verantwortlichen Verwaltungsstellen vorgenommen werden; die Übereinstimmung des Informationsbestandes im Register mit den Informationen in den einzelnen Verwaltungsvorgängen muß sichergestellt werden;
- **fernmündliche** Datenübermittlungen, insbesondere **Auskünfte**, wegen der damit verbundenen Risiken, die anfragende Stelle nicht eindeutig identifizieren und die Übermittlungsbefugnis nicht wirklich prüfen zu können, generell nicht zulässig sein;
- die Zulassung zum **automatisierten Abrufverfahren** besonders kritisch geprüft werden; das Gesetz fordert die Berücksichtigung schutzwürdiger Interessen der Betroffenen und damit eine Rechtsgüterabwägung; die **Nachrichtendienste** sollten gar nicht zugelassen werden;
- die **„Gruppenauskunft"** auf konkrete Straftatbestände beschränkt und so konkretisiert werden, daß die Voraussetzungen der Strafprozeßordnung für Rasterfahndungsmaßnahmen zugrunde zu legen sind.

Der Bundesinnenminister hat unsere Vorschläge bisher nicht berücksichtigt. Es bleibt zu hoffen, daß Schleswig-Holstein im Bundesrat unsere Vorschläge unterstützt.

4.1.3.4 Asylcard

Nach Banken und Versicherungen entdeckt auch die Verwaltung die intelligente Chipkarte für sich. Bei den Asylbewerbern soll eine Smartcard erprobt werden, auf der umfangreiche Daten gespeichert sind.

Neben der Beratung einer Durchführungsverordnung zum Ausländerzentralregistergesetz werden inzwischen auch schon Fragen der Harmonisierung, Rationalisierung und Verbesserung des Asylverfahrens diskutiert. Dort wird die Meinung vertreten, eine größtmögliche Verfahrensoptimierung durch Einführung einer sogenannten **Asylcard** erreichen zu können. Dabei hat man ein intelligentes Identifikationspapier mit integriertem Prozessorchip im Sinn, das neben **Lichtbild** und **biometrischen Daten** des Fingerabdrucks auch wesentliche Verfahrensdaten eines Asylbewerbers enthalten soll. Die Karte soll unter anderem der Identifizierung des Trägers, der Kontrolle von Aufenthalt und Zutritt sowie des Empfangs von Sach- und Unterstützungsleistungen dienen. Gespeichert werden sollen auch Arbeitserlaubnisse und weitere, noch festzulegende Informationen.

In einer ersten Stellungnahme gegenüber dem Innenminister haben wir erhebliche **Vorbehalte** geltend gemacht. Abgesehen von einer Fülle technischer und verfahrensmäßiger Probleme stellt sich in erster Linie die Frage der verfassungsrechtlichen Zulässigkeit. Das Bundesverfassungsgericht hat die automatisierte Herstellung von **Persönlichkeitsprofilen** für unzulässig erklärt.

Der Grundsatz der **Zweckbindung** steht einer Nutzung personenbezogener Daten für beliebige Zwecke, so wie eine multifunktionale Chipkarte sie ermöglicht, entgegen.

Unsere Kritik an der unterschiedslosen erkennungsdienstlichen Behandlung aller Asylbewerber und Bürgerkriegsflüchtlinge (vgl. 15. TB, S. 36 f.) wird verstärkt durch die jetzt vorgesehene **Speicherung** des **Fingerabdrucks** in der Asylcard.

Auch eine Reihe weiterer Bedenken spricht gegen die Einführung der Asylcard (vgl. auch Tzn. 4.8.1, 7.2). Wir haben den Innenminister gebeten, unsere Hinweise bei den weiteren Beratungen zu unterstützen.

4.2 Umweltschutz

Privatisierung der Abfallentsorgung kann den Datenschutz der Bürger gefährden.

Will sich ein Kreis oder eine kreisfreie Stadt einer privaten Firma zur Müllentsorgung bedienen, so müssen die Verträge die Kriterien der Auftragsdatenverarbeitung erfüllen. Sollen personenbezogene Daten erhoben werden, so ist dies präzise in der Abfallgebührensatzung zu regeln.

In zunehmendem Maße bedienen sich Kreise und Städte bei der Müllentsorgung **privater Abfallwirtschaftsunternehmen**. Dabei sind aus datenschutzrechtlicher Sicht zwei Gesichtspunkte zu unterscheiden:

Zum einen soll das private Unternehmen die physikalisch-technische **Beseitigung der Abfälle** (Einsammlung, Verbrennung usw.) für die abfallentsorgungspflichtige Körperschaft durchführen und zum anderen für den betreffenden Kreis auch die **Gebührenerhebung** vornehmen.

Das Abfallgesetz des Bundes (AbfG) und das Abfallwirtschaftsgesetz des Landes (LAbfWG) sehen **keine Übertragung** der öffentlich-rechtlichen **Aufgabe** „Abfallbeseitigung" auf private Dritte vor. Eine private Abfallwirtschaftsgesellschaft kann also nicht als „beliehener Unternehmer" auftreten, sondern nur als privater Auftragnehmer.

Die Befugnis, von den Bürgern die erforderlichen personenbezogenen Daten zu erheben, haben also nur die Kreise. Für die Gebührenerhebung gelten die Vorschriften des schleswig-holsteinischen Kommunalabgabengesetzes (KAG).

Bei der damit in Zusammenhang stehenden Datenverarbeitung sind die strengen Voraussetzungen des Landesdatenschutzgesetzes zur **Auftragsdatenverarbeitung** zu beachten.

Es muß also vertraglich klar geregelt sein, daß die Abfallwirtschaftsgesellschaften

- die Daten nur nach **genauen Anweisungen** des Kreises verarbeiten,
- die **notwendigen Datensicherungsmaßnahmen** treffen und
- **Kontrollen** jederzeit möglich sind.

Beschwerden der Bürger zeigen, daß die Behörden ihrer Verantwortung für die personenbezogenen Daten nicht immer gerecht werden, wenn sie diese von einer Privatfirma im Auftrage verarbeiten lassen.

4.3 Kommunalbereich

4.3.1 Kontrollergebnisse aus den Kommunen

Kontrollen bei einer Kommunalverwaltung haben erneut datenschutzrechtliche Mängel ergeben. Die betroffene Stadt hat rasche Mängelbeseitigung in Aussicht gestellt.

Die letztjährigen Prüfungsergebnisse im kommunalen Bereich (vgl. 16. TB, S. 37 ff.) hatten Mängel bei der Aufnahme von Datenverarbeitungsregelungen in das Satzungsrecht sowie in der Handhabung des Aufklärungsgebots bei der Datenerhebung aufgezeigt. Im Berichtsjahr wurde deshalb erneut eine Prüfung im Bereich der kommunalen Selbstverwaltungsaufgaben durchgeführt.

Allgemeine Feststellungen

Die **Ergebnisse** waren erneut **unbefriedigend**. Zwar waren für die Selbstverwaltungsbereiche **Datenverarbeitungsvorschriften** erlassen worden, sie entsprachen jedoch nicht den gesetzlichen Anforderungen. **Zu beanstanden** war insbesondere, daß

- Datenverarbeitung in einem Umfang zugelassen wurde, der zur rechtmäßigen Aufgabenerfüllung nicht erforderlich war,
- Befugnisse zur Datenverarbeitung nicht hinreichend präzise festgelegt waren,
- die in der Satzung beschriebene Verarbeitung personenbezogener Daten nicht mit den tatsächlichen Verhältnissen übereinstimmte,
- die tatsächliche Datenverarbeitung, z.B. im Hinblick auf die Aufklärung der Betroffenen bei der Datenerhebung, nicht mit den gesetzlichen Vorschriften übereinstimmte,
- die in Akten gespeicherten Daten zu lange aufbewahrt wurden.

Wir haben u.a. empfohlen, in einer **Aktenordnung** nähere Regelungen zur Aufbewahrungsfrist zu treffen, die dem vom Datenschutzgesetz vorgeschriebenen Begriff der Erforderlichkeit gerecht werden.

Datenverarbeitung im Alten- und Pflegeheim

Die Verwaltung des Bargeldes der Heimbewohner erfolgte in einer Reihe von Fällen ohne wirksame Vollmacht der Betroffenen. In einem Fall war dem Kreissozialamt sogar der Stand eines Bargeldkontos mitgeteilt worden, um überprüfen zu lassen, ob der Heimbewohner die ihm nach dem Bundessozialhilfegesetz gezahlten Barbeträge bestimmungsgemäß verwendet hatte. Der Betroffene hatte von der Mitteilung erst nach der Einstellung der Leistungen des Kreissozialamtes Kenntnis erhalten.

In den Verwaltungsakten des Heimes befand sich auch privater Schriftwechsel der Bewohner, der im Rahmen der persönlichen Betreuung vom Hause mit verwaltet wurde. Wegen der besonderen Zweckbindung dieser Unterlagen wurden die Vorgänge auf unsere Veranlassung hin getrennt.

Erstellung von Wegzugslisten des Meldeamtes

Bei der Prüfung der Stadtbücherei stellte sich heraus, daß die **Kundendatei regelmäßig** aufgrund von Wegzugslisten des Meldeamtes **aktualisiert** wurde. Auf Nachfrage bestritten die Mitarbeiter des Meldeamtes wie auch der Ordnungsamtsleiter ausdrücklich die Herausgabe solcher Listen.

Weitere Nachforschungen ergaben dann, daß entsprechende Listen vom **Systembetreuer der EDV-Anlage ohne Kenntnis** des **Ordnungsamtes** erstellt und nicht nur der Bücherei, sondern auch dem Sozialamt zur Verfügung gestellt worden waren. Eine Weisung zur Erstellung der Listen lag nicht vor. Mit der eigenverantwortlichen Erstellung der Listen hatte der Systembetreuer den Rahmen der ihm übertragenen Aufgaben weit überschritten. Ermöglicht wurde der Verstoß durch eine nicht ausreichende Kontrolle des Systembetreuers und der Datenübermittlungen innerhalb der Stadtverwaltung.

Einziehung von Forderungen im Rahmen der Gegenseitigkeitshilfe der Stadtwerke

Wenn der Inhaber eines Versorgungsanschlusses verzogen war, ohne seine Rechnung vollständig zu bezahlen, bedienten sich die Stadtwerke einer sogenannten **Gegenseitigkeitshilfe**. Das Energieversorgungsunternehmen am neuen Wohnort des Schuldners wurde gebeten, „den Kunden zur Zahlung zu bewegen". Weiter hieß es in entsprechenden Schreiben: „Sollten Ihre Bemühungen nicht zum Erfolg führen, wären wir für Hinweise über Einkommens- und Vermögensverhältnisse un-

seres Schuldners sowie für die Angabe seines Arbeitgebers dankbar."

Bei der Gegenseitigkeitshilfe wurden sowohl an öffentliche wie auch private Stellen besonders geschützte Vertragsdaten unzulässigerweise übermittelt. Auf unsere Beanstandung hin wurde die Praxis eingestellt.

Unterrichtung des Magistrats über Entscheidungen zur Nichtausübung des Vorkaufsrechts

Auf Beschluß des Magistrats waren ihm grundsätzlich nur die Kaufverträge zur Entscheidung vorzulegen, in denen tatsächlich ein gesetzliches Vorkaufsrecht ausgeübt werden sollte. Die **Entscheidung** über den Verzicht auf das Vorkaufsrecht war auf den **Leiter der Bauverwaltung** bzw. dessen Vertreter **delegiert** worden. Über diese Fälle wurde der Magistrat im nachhinein unter Vorlage der vollständigen Kaufverträge informiert.

Zum Zeitpunkt der Unterrichtung der Magistratsmitglieder war die abschließende **Entscheidung** über die Ausübung des Vorkaufsrechts **bereits getroffen** worden. Die Vorlage der Kaufverträge war also nicht mehr erforderlich.

Überdies wurden eingehende Kaufverträge in einer Liste unter Angabe des Verkäufers, des Käufers, der Größe sowie der Lage des Grundstücks erfaßt und gemeinsam mit den vollständigen Verträgen zumindest seit dem Jahr 1985 aufbewahrt. Für die Führung einer derartigen **Kaufvertragsdatei** besteht im kommunalen Bereich weder eine Befugnis noch eine Notwendigkeit, sie war deshalb zu vernichten. Zur Übermittlung von Kaufverträgen durch Notare gilt in Schleswig-Holstein nunmehr ein neues Verfahren (vgl. Tz. 9.4). Danach erhalten die Kommunen künftig nur noch dann vollständige Verträge, wenn die Ausübung des gesetzlichen Vorkaufsrechts tatsächlich in Betracht kommt.

Reaktion der Stadt

Die Prüfungsanregungen und Beanstandungen wurden von der Stadt aufgegriffen. In ihrer Stellungnahme führt sie aus: „Wir gehen davon aus, Ihre Beanstandungen, Empfehlungen usw. hiermit ausgeräumt bzw. umgesetzt zu haben bzw. dies so bald wie möglich zu realisieren."

4.3.2 Welche personenbezogenen Daten dürfen Gemeindevertreter zur Vorbereitung von Entscheidungen erhalten?

Mitglieder von Gemeindevertretungen und kommunalen Ausschüssen dürfen nur die personenbezogenen Informationen erhalten, die für ihre Entscheidungen erforderlich sind. Werden sensible Punkte behandelt, ist die Öffentlichkeit auszuschließen.

Fast in jedem Berichtsjahr taucht in Eingaben die Frage auf, ob und in welchem Umfang den Gemeindevertretungen und ihren Ausschüssen für die **Vorbereitung von Entscheidungen** personenbezogene Daten zugeleitet und ob diese in Sitzungen erörtert werden dürfen (z.B. Auskünfte über Sozialhilfebezug bei Anträgen auf Befreiung von kommunalen Abgaben, personenbezogene Informationen zur Entscheidung über Gewerbesteuerstundungen, zulässiger Umfang der Unterrichtung von Gemeindevertretern in Bauantragsverfahren).

Vielfach besteht auch Unsicherheit, über welche Informationen in **öffentlichen Sitzungen** beraten werden darf und in welchen Fällen die Öffentlichkeit auszuschließen ist.

Bei der Tätigkeit von Gemeindevertretern ist der **Grundsatz** zu beachten, daß sie über diejenigen **Daten** verfügen müssen, die für die rechtmäßige Aufgabenerfüllung **erforderlich** sind. Hat also die Gemeindevertretung oder ein Ausschuß eine Verwaltungsentscheidung zu treffen, so müssen die Mitglieder die dazu erforderlichen Informationen erhalten. Erforderlich sind Informationen dann, wenn ohne sie eine Entscheidung sachgemäß nicht getroffen werden kann.

Das Sozialgesetzbuch (SGB) verbietet grundsätzlich die Übermittlung von **Angaben zur Sozialhilfe**, soweit sie nicht für die Erfüllung einer gesetzlichen Aufgabe nach dem SGB erforderlich ist. Bei Entscheidungen über die Ermäßigung kommunaler Abgaben dürfen daher ohne Einwilligung der Betroffenen Angaben zum Sozialhilfebezug nicht an die Gemeindevertretungen weitergegeben werden. Allerdings wird die Einwilligung durchweg erreichbar sein, da die Betroffenen die Voraussetzungen für Abgabenermäßigungen nachweisen müssen und der Hinweis auf die Sozialhilfe die einfachste Form des Nachweises sein dürfte.

Ähnliches gilt für den Fall der **Steuerstundung**. Das Steuergeheimnis wird nicht verletzt, wenn die Verantwortlichen für eine Entscheidung im Stundungsverfahren über die erforderlichen Details unterrichtet werden. Dazu gehören jedenfalls der Name des Steuerschuldners, die Höhe des zu stundenden Betrages und die Antragsgründe. Einzelheiten über die wirtschaftlichen Verhältnisse sind nur dann erforderlich, wenn ohne sie die Antragsgründe im Einzelfall nicht geprüft werden könnten.

Auch im Zusammenhang mit **Bausachen** erhält das zuständige Gremium die Daten, deren Kenntnis es für die vorgesehene Entscheidung im Einzelfall bedarf. Daneben kann einzelnen Mitgliedern Auskunft erteilt und u. U. Akteneinsicht gewährt werden, wenn dies für die Vorbereitung oder Kontrolle der Ausführung einzelner Beschlüsse der Gemeindevertretung oder ihrer Ausschüsse erforderlich ist. Es muß also immer ein **Bezug** zu **konkreten Beschlüssen** und **Beschlußvorlagen** vorhanden sein. Nach alledem hängt das Informationsrecht kommunaler Vertreter von der Erforderlichkeit für den einzelnen Entscheidungsgegenstand ab.

Ob die Entscheidung in öffentlicher Sitzung vorbereitet und getroffen werden darf, richtet sich dabei nach den Vorschriften des **kommunalen Verfassungsrechts**, die die Öffentlichkeit von Sitzungen der Gremien regeln. Hier gilt grundsätzlich, daß die **Öffentlichkeit auszuschließen** ist, wenn berechtigte Interessen einzelner es erfordern (z.B. Sozialgeheimnis, Steuergeheimnis, aber auch gewichtige geschäftliche Interessen). Dies hat der Vorsitzende zu prüfen und eine Entscheidung herbeizuführen.

4.3.3 Berichtigungsanspruch bei fehlerhafter Darstellung personenbezogener Daten in Gemeindevertretersitzungen

Werden in einer Sitzung der Gemeindevertretung unrichtige Auskünfte über Bürger erteilt, so ist nicht das Protokoll zu korrigieren, sondern in der nächsten Sitzung eine Richtigstellung vorzunehmen.

Im Rahmen einer **Einwohnerfragestunde** wurden vom Bürgermeister Auskünfte erteilt, die auch Angaben über persönliche und sachliche Verhältnisse des Fragestellers enthielten. Im nachhinein stellten sich diese Angaben als fehlerhaft heraus. Der Betroffene beantragte deshalb unter Berufung auf den datenschutzrechtlichen Berichtigungsanspruch eine Änderung der Darstellung im Sitzungsprotokoll.

Nach unserer Auffassung kam hier eine Berichtigung der Sitzungsniederschrift nicht in Betracht. In einem solchen **Protokoll** soll der **tatsächliche Verlauf der Sitzung** dokumentiert werden. Eine Gewähr für die Richtigkeit von Daten in Redebeiträgen wird nicht übernommen. Eine Berichtigung kommt deshalb nur in Betracht, wenn die in der Sitzung gemachten Ausführungen nicht mit der Darstellung im Protokoll übereinstimmen.

Dagegen bestand jedoch ein **Anspruch** auf **Richtigstellung** der Angaben in der nächsten Gemeindevertretersitzung. Betroffene haben einen **Anspruch** darauf, daß Auskünfte, die von Behörden erteilt werden, **richtig** sind. Stellt sich die Unrichtigkeit personenbezogener Daten heraus, sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. Im konkreten Fall bedeutete dies, daß die unrichtigen Auskünfte in der nächsten **Gemeindevertretersitzung richtiggestellt** werden mußten, so daß die Öffentlichkeit in gleicher Weise wie bei der Bekanntgabe der fehlerhaften Daten davon Kenntnis erhielt. Die Berichtigung ist dann auch im Protokoll nachzulesen.

4.3.4 Wenn die Kindergärtnerin nach dem Einkommen der Eltern fragt

Viele Eltern sehen es mit Unbehagen, wenn sie gegenüber einem privaten Kindergarten ihr Einkommen offenlegen sollen, um in den Genuß einer Gebührenermäßigung zu

kommen. Die Beauftragung der Kommune mit dem Gebühreneinzug kann eine sachgerechte Lösung sein.

In einer Stadt betrieben die Kirchengemeinde und ein privater Trägerverein je einen Kindergarten. Sie hatten keine eigene Regelung über die Benutzungsentgelte beschlossen, sondern eine städtische „Gebührenordnung" übernommen und die **Stadt** mit der Erhebung der Beiträge **beauftragt**. Der Magistrat hatte eine „Gebührenordnung für die Benutzung der Kindertagesstätten in der Stadt ..." beschlossen, obwohl die Stadt gar keinen eigenen Kindergarten betrieb. Interessierte Eltern unterrichtete sie durch ein Informationsblatt über die „Kindergartengebühren 1993/1994". Darin erläuterte sie u.a. die Zusammensetzung des „Nettofamilieneinkommens", Absetzungsmöglichkeiten, Kostenberechnungen, „Gebühren"höhe u.ä.. Das Merkblatt schloß mit den Worten: „Mit freundlichen Grüßen, Ihre Stadtverwaltung ...".

Beigefügt war außerdem ein formularmäßiger „Antrag auf Einstufung in die **Gebührenstaffel** für Kindergärten", mit dem Angaben über das Familieneinkommen interessierter Eltern erhoben werden sollten. Darin hieß es u.a.: „Ich bin/Wir sind damit einverstanden, daß die zur Einkommens- und Absetzungsberechnung notwendigen Unterlagen und Sozialdaten beim Sozialamt der Stadt ... verarbeitet und gespeichert werden. Die automatisierte Verarbeitung ist zulässig. Diese Zustimmung erstreckt sich nur auf die Einkommens-/Absetzungsberechnung im Rahmen der Einstufung in die Sozialstaffel."

Im konkreten Fall war also die **Stadt Auftragnehmer** für die Datenverarbeitung der Träger der privaten Kindergärten. Die Stadt erhob daher die personenbezogenen Daten nicht auf der Grundlage ihrer eigenen Satzung. Maßgebende Grundlagen für das Verfahren waren vielmehr die Verträge der Eltern mit den Kindergartenträgern in Verbindung mit deren Beschlüssen zur Beauftragung der Stadt mit dem Gebühreneinzug.

Bedenken ergaben sich aus unserer Sicht gegen die Art, in der die Eltern über das Verfahren unterrichtet wurden. Weder vom Druckbild her, noch was die Hinweise auf die Rechtsgrundlage und den Zweck der Verarbeitung betrifft, war das Antragsformular in Ordnung. Es fehlte auch ein Hinweis, daß die Stadt hier nicht hoheitlich, sondern im Auftrag privater Stellen tätig war.

Werden diese Schwächen behoben, ist gegen die Beauftragung der Stadt mit dem Gebühreneinzug und der damit verbundenen Datenverarbeitung nichts einzuwenden. Denn aus einer Reihe von Einzeleingaben ist uns bekannt, daß viele Eltern ihre Einkommensverhältnisse lieber vor einer öffentlichen Stelle als etwa vor der Leitung eines privaten Kindergartens offenlegen.

4.3.5 Kontrolle gaststättenrechtlicher Erlaubnisverfahren

Bei einer Prüfung wurden Mängel bei den gaststättenrechtlichen Erlaubnisverfahren festgestellt. Datenschutzrechtliche Mindeststandards waren weitgehend unbekannt.

Im Rahmen einer Prüfung gaststättenrechtlicher Erlaubnisverfahren haben wir folgende datenschutzrechtliche Mängel festgestellt:

Anforderung von Lebensläufen

Im Rahmen der Antragstellung für Gaststättenerlaubnisse wurden von den Betroffenen **Lebensläufe gefordert**. Zusätzlich wurden in dem landeseinheitlichen Antragsformular ganz allgemein Angaben über den Aufenthalt und die berufliche Betätigung in den letzten drei Jahren vor Antragstellung verlangt.

Die bei unserer Kontrolle vorgefundenen Lebensläufe differierten inhaltlich erheblich. Teilweise wurden Angaben über Eltern und Geschwister gemacht, in einem anderen Fall wurden die einzelnen Phasen der Schulausbildung detailliert dargelegt. Dagegen enthielt der kürzeste Lebenslauf neben den Angaben zur Person nur folgende Aussage: „Ich bin seit 1981 in Deutschland und habe immer in der Gastronomie gearbeitet". Auch diese Kurzfassung reichte offensichtlich für die Erteilung der Gaststättenerlaubnis aus.

Für die Betroffenen war bei einer so **unspezifizierten Datenanforderung** wie einem „Lebenslauf" nicht erkennbar, welche ihrer Daten wirklich für die Entscheidung benötigt wurden. Um sich nicht dem Vorwurf auszusetzen, einen unvollständigen Lebenslauf abgegeben zu haben, wurden häufig mehr Angaben gemacht als tatsächlich erforderlich waren. Die vorgefundenen Lebensläufe enthielten deshalb in der Regel auch eine Vielzahl von Daten, die für die beantragte Erlaubnis nicht entscheidungsrelevant waren. Soweit Angaben über frühere Aufenthalte und berufliche Betätigungen der Betroffenen benötigt wurden, wären diese Daten präzise über das vorgeschriebene Antragsformular zu erfragen gewesen. Für einen weitergehenden Lebenslauf besteht keine Notwendigkeit.

Einholung eines Führungszeugnisses

In einem der geprüften Fälle war im Erlaubnisverfahren versäumt worden, vom Antragsteller ein **Führungszeugnis über die Ehefrau** zu fordern. Als dies ca. ein Jahr nach Erlaubniserteilung festgestellt wurde, füllte die geprüfte Stelle eigenmächtig einen „Antrag einer Privatperson auf Erteilung eines Führungszeugnisses" aus, bestätigte anschließend die Angaben als Meldebehörde und veranlaßte schließlich die Zustellung der Rückantwort unmittelbar an die Ordnungsbehörde. Eine Unterschrift der Betroffenen war im Antragsformular nicht vorgesehen. Der **Antragsteller** und seine **Ehefrau** hat-

ten von diesem Vorgang **keine Kenntnis**. Sie wurden darüber erst unterrichtet, als von ihnen im nachhinein die Zahlung einer **Verwaltungsgebühr** verlangt wurde.

Das **Bundeszentralregistergesetz** läßt eine Auskunft an Behörden nur zu, wenn sie für die Erfüllung einer hoheitlichen Aufgabe benötigt wird und eine Anforderung über den Betroffenen nicht sachgemäß ist oder erfolglos bleibt. Diese Voraussetzungen waren hier nicht erfüllt. Die beantragte Erlaubnis war rechtskräftig erteilt worden. Es waren nur eben die Akten nicht „vollständig".

Vorrang der Datenerhebung beim Betroffenen

Vor Erteilung von Erlaubnissen wurden regelmäßig die **örtlichen Ordnungsbehörden** der Gemeinden, in denen der Antragsteller bzw. sein Ehegatte in den letzten drei Jahren vor Antragstellung ihren Wohnsitz hatten zur persönlichen Zuverlässigkeit der Betroffenen gehört.

Die Anhörung der örtlichen Ordnungsbehörden ist zwar in den Verwaltungsvorschriften zum Gaststättengesetz vorgesehen. Das Landesdatenschutzgesetz und inzwischen auch die Gewerbeordnung schreiben jedoch einen **Vorrang der Datenerhebung beim Betroffenen** vor.

Nach unserer Auffassung hätten die Betroffenen aufgefordert werden müssen, eine **„ordnungsrechtliche Unbedenklichkeitsbescheinigung"** selbst beizubringen. Eine Datenerhebung durch die geprüfte Stelle wäre allenfalls als Serviceleistung auf besonderen Wunsch der Antragsteller zulässig gewesen.

Regelmäßige Datenerhebung bei örtlichen Polizeidienststellen

Zur Prüfung der persönlichen Zuverlässigkeit wurden außerdem regelmäßig **Anfragen** an die für den Wohnsitz zuständige **Polizeidienststelle** gerichtet. Dies war für die Aufgabenerfüllung der geprüften Stelle nach den von uns getroffenen Feststellungen **nicht erforderlich**. Eine regelmäßige Beteiligung örtlicher Polizeidienststellen ist selbst in den Verwaltungsvorschriften des Wirtschaftsministers nicht vorgesehen. Zur Gewährleistung einer umfassenden Zuverlässigkeitsprüfung könnten ggf. Angaben über schwebende Verfahren vom Antragsteller verlangt werden. Stellt sich später z.B. durch eine „Mitteilung in Strafsachen" heraus, daß unrichtige oder unvollständige Angaben gemacht worden sind, kann eine rechtskräftig erteilte Erlaubnis nach den Vorschriften des Landesverwaltungsgesetzes zurückgenommen werden.

Aufklärung der Betroffenen bei der Datenerhebung

Bei der Bearbeitung eines Antrages werden in erheblichem Umfang weitere personenbezogene Daten erhoben. Die Be-

troffenen waren darüber in allen geprüften Fällen **nicht aufgeklärt** worden. Auch eine Unterrichtung über die Beteiligung anderer Stellen am laufenden Verfahren war nicht erfolgt.

Routinemäßige Unterrichtung der Polizei

Nach Erteilung einer Gaststättenerlaubnis erhielt die örtliche Polizeidienststelle jeweils eine **Durchschrift des Bescheides** zur Kenntnis. Der genaue Zweck, zu dem die Unterrichtung erfolgte, konnte von der geprüften Stelle nicht genannt werden, aber das habe man schon immer so gemacht.

Für den Betrieb einer Gaststätte ist keine besondere Überwachung durch die Polizei vorgeschrieben. Es mußte deshalb davon ausgegangen werden, daß die Übermittlung der Daten nicht zur Erfüllung der Aufgaben nach dem Gaststättengesetz erfolgte. Eine ausreichende Befugnisgrundlage war dafür nicht vorhanden. Die Datenübermittlung war deshalb zu beanstanden.

Speicherung personenbezogener Daten in Erlaubnisakten

Die Führung der Akten erfolgte „objektbezogen". Es wurden alle Unterlagen, die eine bestimmte Gaststätte betrafen, in einem Vorgang dauerhaft aufbewahrt. Eine Prüfung, ob die jeweiligen Unterlagen entscheidungserheblich waren, fand nicht statt. Dies führte z.B. dazu, daß im Rahmen der Prüfung der persönlichen Zuverlässigkeit eine von der Kriminalpolizei in Kopie übersandte **Strafanzeige** gespeichert wurde, die erhebliche Vorwürfe gegen den Antragsteller enthielt. Dieser Strafanzeige war u.a. die Behauptung zu entnehmen, der Betroffene habe einem früheren Konkurrenten gedroht, „er werde ihn alle machen, damit er sein Maul nie wieder aufreißen könne". Gleichwohl war das **Strafverfahren** ohne weitere Aufklärung des Sachverhalts mangels öffentlichen Interesses **eingestellt** worden.

Ob der Sachverhalt bei der Entscheidungsfindung der geprüften Stelle berücksichtigt wurde, war den Akten nicht zu entnehmen. Die **Erlaubnis** wurde jedenfalls **vorbehaltlos erteilt**. Fraglich blieb, zu welchem Zweck die Kopie der Strafanzeige gespeichert wurde, da weder eine Sachverhaltsaufklärung noch eine Anhörung des Betroffenen erfolgte.

In Erlaubnisakten dürfen nach dem Landesverwaltungsgesetz nur Unterlagen aufgenommen werden, die von ihrer Zweckbestimmung her **zur Dokumentation** der zu treffenen Verwaltungsentscheidung **erforderlich** sind. Nur auf diese Weise können Betroffene bei einer Akteneinsicht erkennen, welche Sachverhalte für ihr Erlaubnisverfahren von Bedeutung sind. Deshalb muß vor Aufnahme eines Vorgangs in die Erlaubnisakte der darin enthaltene Sachverhalt ausreichend geklärt und erlaubnisrechtlich gewichtet werden. In den geprüften Akten war dies zumindest nicht ausreichend dokumentiert.

4.4 Justizverwaltung

4.4.1 GAST

Für das staatsanwaltschaftliche System zur Geschäftsstellenautomation (GAST) existiert noch immer keine Rechtsgrundlage. Der Übergangsbonus ist nach unserer Ansicht abgelaufen.

Bereits in den letzten Tätigkeitsberichten (vgl. z.B. 16. TB, S. 43) hatten wir zur fehlenden Rechtsgrundlage für das GAST-System Stellung genommen. An der dort beschriebenen Situation hat sich bis heute nichts geändert. Nach wie vor werden in GAST die Daten der Personen gespeichert, gegen die in Schleswig-Holstein ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Für diesen hochsensiblen Datenbestand gibt es keine Rechtsgrundlage. Mit dem Ablauf der 12. Legislaturperiode des Deutschen Bundestages dürfte auch der sogenannte **„Übergangsbonus" abgelaufen** sein.

Auch wenn einige Gerichte in den vergangenen Jahren den Übergangsbonus noch bejaht hatten, so kann dieser Zustand nicht zu einer Quasi-Rechtsgrundlage auf Dauer umgedeutet werden. Fraglich erscheint überdies, ob aus dieser Richtung weiterhin mit Schützenhilfe für die Staatsanwaltschaft gerechnet werden kann. So hatte das **OLG Frankfurt** bereits 1987 in einer Entscheidung zu den zentralen Namenskarteien der Staatsanwaltschaften in Hessen ausgeführt: „Diese Frist ist jedoch zu begrenzen. Als geeigneter Anknüpfungspunkt kommt das **Ende der laufenden Legislaturperiode** des Deutschen Bundestages **im Jahre 1990** in Betracht."

Auch das **Schleswig-Holsteinische Oberlandesgericht** ging im März 1993 noch von einer Fortdauer des Übergangsbonus aus, konnte dies jedoch nur noch mit vorrangigem Gesetzgebungsbedarf anläßlich der Deutschen Einheit sowie der zwingenden Erforderlichkeit dieser Daten für eine effektive Strafverfolgung begründen.

Derselbe Senat des **OLG Frankfurt**, der den Übergangsbonus bis 1990 befristet hatte, sah sich im Jahre 1994 erneut mit dieser Frage befaßt. Zur Begründung, warum der von ihm selbst gesetzte Ablaufzeitpunkt nicht zu einer Rechtswidrigkeit der zentralen Namenskarteien führte, zog das Gericht u.a. auch die Argumente des Schleswiger Urteils heran. Doch auch hier machte das Gericht deutlich, daß an eine endlose Ausdehnung des Übergangsbonus nicht zu denken ist. Es ging vielmehr zum Entscheidungszeitpunkt (am 19.05.1994) davon aus, es sei vertretbar, „bei zügiger Weiterverfolgung des jetzigen Gesetzesvorhabens der Länder die Übergangsfrist (noch) nicht als abgelaufen anzusehen". Außerdem müßten die Vorschläge der Datenschutzbeauftragten in die Gesetzgebung einfließen.

Von einer „zügigen" Weiterarbeit an der Vorlage der Bundesländer und ihrer datenschutzrechtlichen Verbesserung kann jedoch keine Rede sein. Statt dessen wurde der bis dahin

vorliegende, ohnehin inakzeptable Entwurf weiter verschlechtert und kurz vor Ende der Legislaturperiode mit der Stimme Schleswig-Holsteins als Bundesratsentwurf eingebracht. Dieser Entwurf, der datenschutzrechtlich jeder Beschreibung spottet, schmort nunmehr in den Gremien.

Statt dessen wurden inzwischen Vorschriften über die Errichtung eines **bundeseinheitlichen staatsanwaltschaftlichen Informationssystems** verabschiedet. Darin werden die Rechtsgrundlagen für ein Register aller in der Bundesrepublik geführten und noch nicht abgeschlossenen Ermittlungsverfahren gelegt. Der Bund hat also insoweit von seiner Gesetzgebungskompetenz Gebrauch gemacht, aber ein ganz anderes System als GAST zugelassen. Er hat sich dafür entschieden, das derzeitige GAST-Verfahren nicht auf eine bundesrechtliche Grundlage zu stellen, sondern ausschließlich einen bundesweiten Überblick über alle anhängigen Ermittlungsverfahren zuzulassen. Da GAST weit darüber hinausgeht und auch die Daten von abgeschlossenen Ermittlungsverfahren enthält, stehen die neuen bundesrechtlichen Vorschriften GAST sogar entgegen. In dieser Situation ist nach unserer Auffassung eine weitere Berufung auf den „Übergangsbonus" nicht möglich.

Nach diesen Erfahrungen mit GAST verdienen die **neuen Automationsvorhaben** des Justizministers (vgl. Tz. 4.4.2) besondere Beachtung. Es ist hier nachdrücklich davor zu warnen, mit Millionenaufwand weitere Systeme ohne Rechtsgrundlage zu schaffen. Ein Übergangsbonus steht für neue Verfahren nicht zur Verfügung!

Da nach den Erfahrungen in den vergangenen 12 Jahren und nach der Entscheidung für ein andersgeartetes bundesweites staatsanwaltschaftliches Verfahren vom Bundesgesetzgeber keine schnelle Hilfe mehr erwartet werden kann, muß nun der **schleswig-holsteinische Gesetzgeber** endlich handeln.

4.4.2 Neue Automationsvorhaben der Justiz

Unter der Bezeichnung „Staatsanwaltschaft 2000" werden die Staatsanwaltschaften flächendeckend mit vernetzten Personalcomputern ausgestattet. Für die Gerichte wird das Automationssystem „MEGA" entwickelt.

Mit hohem finanziellem Aufwand bemüht sich der Justizminister, in allen Arbeitsbereichen der Justiz neue Ressourcen durch erweiterte EDV-Unterstützung zu gewinnen. So werden in absehbarer Zeit **alle Staatsanwälte** des Landes über **Arbeitsplatzrechner** verfügen, mit deren Hilfe sie nicht nur Textverarbeitung betreiben, sondern auch andere Formen der EDV-gestützten verfahrensbegleitenden Bearbeitung durchführen können.

Dieselben Bestrebungen laufen bei den **Gerichten**. Dort soll nun eine automatisierte Unterstützung für die Geschäftsstellen geschaffen werden. Bei dem neuen Konzept wird besonderer

Wert auf die vollständige Integration auch des Richterarbeitsplatzes gelegt.

Es stellt sich zunächst die Frage nach den **Rechtsgrundlagen**. Seit Jahren weisen wir auf die fehlenden gesetzlichen Vorschriften für das GAST-System hin (vgl. Tz. 4.4.1). Ebensowenig wie die Strafprozeßordnung enthalten die anderen Prozeßordnungen Vorschriften, die unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts die Verarbeitung personenbezogener Daten umfassend und präzise regeln. Nach der neuen Datenschutzverordnung kann ein Automationsvorhaben nur dann als ordnungsgemäß angesehen werden, wenn es auf einwandfreien gesetzlichen Grundlagen beruht. Mit den derzeitigen Investitionen im Justizbereich geht das Land jedenfalls dann ein Risiko ein, wenn mit der Automatisierung auch neuartige Nutzungen verbunden sind.

4.4.3 Strafakten werden zu lange aufbewahrt

Auch die Aufbewahrung hochsensibler Informationen aus Straf- oder anderen Prozessen in Akten greift in das informationelle Selbstbestimmungsrecht der Bürger ein. Gesetzliche Vorschriften darüber, wie lange solche Vorgänge aufzubewahren sind, existieren jedoch nicht.

Nicht nur für die Löschung personenbezogener Daten in Dateien und EDV-Systemen gilt der Grundsatz „so früh wie möglich", sondern auch für die **Vernichtung von Akten**. Die Verwaltungsanweisungen der Justiz enthalten zwar **Fristen** für die Aktenvernichtung, diese sind jedoch in zahlreichen Fällen viel zu lang. So werden z.B. unterschiedslos alle Entscheidungen, in denen auf Strafe erkannt worden ist, mindestens 30 Jahre aufbewahrt, unabhängig davon, ob es um eine geringe Geldstrafe oder eine lange Freiheitsstrafe geht.

Spezielle Regelungen für Schleswig-Holstein sind bisher vom **Justizminister** und vom **Generalstaatsanwalt** mit der Begründung abgelehnt worden, hier sei eine **bundesweite Einigung erforderlich**. Es ist jedoch aus unserer Sicht nicht einzusehen, daß man nunmehr über viele Jahre diskutiert und nicht zu einem Ergebnis kommt, obwohl die datenschutzrechtlichen Anforderungen auf dem Tisch liegen. Hierbei handelt es sich im wesentlichen um folgende Punkte:

- Die Aufbewahrungsfristen müssen auf ihre **Erforderlichkeit** überprüft werden. Dabei sind das Recht auf informationelle Selbstbestimmung und das Resozialisierungsinteresse der Betroffenen angemessen zu berücksichtigen.
- Bei der Festlegung der Fristen muß stärker **differenziert** werden. Es geht nicht an, daß die Speicherfrist für den Diebstahl von geringwertigen Sachen gleich lang ist wie bei einem Kapitaldelikt.
- Bei der Berechnung der **Speicherfrist** muß an den Termin der **Rechtskraft** der Entscheidung angeknüpft werden und

nicht wie bisher an die letzte aktenmäßige Bearbeitung des Falles.

- Bei ausnahmsweiser Speicherung trotz **Freispruchs** oder **Einstellung** des Verfahrens sind besondere Schutzvorkehrungen zu treffen, damit nicht durch die Speicherung der Verdacht aufrechterhalten wird.
- Bei Akten, die mehrere Täter betreffen, muß bei der Berechnung der Speicherfristen differenziert werden. Gegebenenfalls sind Aktenteile nach Ablauf einer (Teil-)Speicherungsfrist zu **sperren**.

4.5 Steuerverwaltung

4.5.1 Sicherheitsmängel in der Aktenverwaltung der Finanzämter werden zur „unendlichen Geschichte"

Am fehlenden Geld scheitern bislang als notwendig erkannte Sicherungsmaßnahmen zur Wahrung des Steuergeheimnisses.

Die Prüfungsberichte datieren vom Februar 1993. Unsere **Forderung**, die in mehreren Finanzämtern festgestellten Sicherheitsmängel in der Aktenverwaltung abzustellen und generelle Regelungen für die Finanzämter zu erlassen, wurde von der Oberfinanzdirektion im März 1993 **vom Grundsatz her akzeptiert** (vgl. 16. TB, S. 49). Im November des gleichen Jahres wurde der Entwurf einer Weisung an die Finanzämter vorgelegt. Dieser entsprach aber weder unseren Vorstellungen noch vermochte der Personalrat seine Zustimmung im Rahmen des Mitbestimmungsgesetzes zu geben.

Die Folge ist, daß zwei Jahre nach Abschluß der Prüfungen die festgestellten **Sicherheitsmängel noch immer nicht beseitigt** sind:

- Steuerakten liegen nach Dienstschluß der Mitarbeiter unverschlossen in den Büros.
- Es ist nicht in allen Finanzämtern zwingend vorgeschrieben, Büroräume zu verschließen (und den Schlüssel abzuziehen), wenn sie nicht besetzt sind.
- Es gibt keine Regelung über die ordnungsgemäße Verwahrung von Steuerakten durch Außendienstmitarbeiter.

Der Grund für das zögerliche Verhalten der Oberfinanzdirektion ist inzwischen deutlich geworden: Es liegt am Geld. Steuergeheimnis hin – Steuergeheimnis her, die zur Wahrung dieses ansonsten von der Verwaltung so hoch gehaltenen Rechtsgutes erforderlichen Vorkehrungen dürfen offenbar nicht zuviel kosten. So scheitert z.B. die auch von den Fachreferaten des Ministeriums für erforderlich gehaltene Beschaffung von verschließbaren Aktentaschen für die Außendienstarbeiter am Veto des Finanzministeriums.

Verständlicherweise haben die **Personalräte** dem Entwurf einer **Datensicherheitsanweisung** an die Finanzämter ihre **Zustimmung versagt**, weil in ihr zwar die Sicherungsziele formuliert werden, aber dem nachgeordneten Bereich nicht gesagt wird, mit welchen (finanziellen) Mitteln sie erreicht werden sollen.

Aus unserer Sicht ist es nicht akzeptabel, daß notwendige Maßnahmen zur Wahrung des Steuergeheimnisses auf Dauer davon abhängig gemacht werden, daß sie nichts kosten.

4.5.2 Kirchensteuermerkmale auf Lohnsteuerkarten – „das haben wir immer so gemacht"

Die Notwendigkeit von Kirchensteuermerkmalen auf Lohnsteuerkarten hält einer kritischen Überprüfung nicht stand. Erste Verfahrensänderungen wurden jetzt erreicht.

Solange es das Lohnsteuerabzugsverfahren gibt, enthalten die Lohnsteuerkarten, die den Arbeitgebern vorgelegt werden, neben dem Namen und der Anschrift des steuerpflichtigen Arbeitnehmers sowie der Steuerklasse und der Anzahl der steuerlich zu berücksichtigenden Kinder auch Angaben über die **Zugehörigkeit** zu einer „steuerberechtigten" **Kirche** und zwar sowohl für den **Arbeitnehmer** als auch für seinen **Ehepartner**.

Als die Datenschutzbeauftragten erstmals die Frage stellten, warum die Arbeitgeber wissen müßten, ob die Ehefrau eines Mitarbeiters der evangelischen, der katholischen oder gar keiner Kirche angehört, war die **Antwort des Bundesfinanzministeriums** und der Kirchen durchaus wortreich, aber **nicht überzeugend**. Es hieß, dies sei zu Kontroll- und zu Abrechnungszwecken erforderlich und werde seit jeher ohne Beanstandungen der Betroffenen so praktiziert.

Bei den Datenschutzbeauftragten gingen aber immer wieder **Beschwerden von Bürgern** ein. Auf erneutes Nachfragen stellte man mit einem Mal fest, daß in der Praxis gar keine Kontrollen durchgeführt werden und daß sie zudem höchst ineffektiv wären. Es ging nämlich nur um einen Abgleich der Eintragungen in der Lohnsteuerkarte mit den Angaben in der Steuererklärung. Der ist aber ohnehin nicht möglich, wenn keine Erklärung abgegeben wird bzw. wenn keine Arbeitnehmereinkünfte vorliegen.

Auch das **Abrechnungsargument** erwies sich nur für einen Spezialfall als stichhaltig. Nur wenn ein Ehepartner der einen und der andere Ehepartner der anderen Kirche angehört, teilen sich die beiden Kirchen die gezahlten Steuern. Der Arbeitgeber muß deshalb jeweils 50 % des Betrages in die jeweiligen Spalten der dem Finanzamt zu übersendenden Lohnsteueranmeldung eintragen. Selbst die Notwendigkeit dieses Halbteilungsverfahrens kann man bezweifeln. Jedenfalls befassen sich laut Auskunft des Bundesfinanzministeriums die Kirchensteuer-Referatsleiter zur Zeit mit dieser Frage.

Zunächst ist jedoch folgendes **Ergebnis erreicht**:

„Auf den Lohnsteuerkarten wird in Zukunft nur noch die Konfessionszugehörigkeit des Arbeitnehmers vermerkt. Über den Ehepartner enthält sie nur noch dann eine Angabe, wenn es sich um eine konfessionsverschiedene Ehe handelt (z.B. „ev/rk").

Die Angestellte einer kirchlichen Einrichtung wird also nicht mehr vom Finanzamt dazu „gezwungen", ihrem Arbeitgeber per Lohnsteuerkarte zu offenbaren, daß ihr Mann aus der Kirche ausgetreten ist. Vielleicht wird sie es den Datenschutzbeauftragten danken.

4.6 Wirtschaft, Technik und Verkehr

4.6.1 Datenschutzrechtliche Mängel bei Führerscheinstellen beanstandet

Bei vielen Führerscheinstellen werden belastende Informationen über Jahrzehnte aufbewahrt, auch wenn sie durch Aktenrückhalt nicht mehr belegt werden können und im Bundes- und Verkehrszentralregister längst gelöscht sind. Auch im übrigen bedarf die Datenverarbeitungspraxis in diesen Stellen dringend der datenschutzrechtlichen Revision.

Ausgelöst durch Eingaben und die Diskussion um die Änderung des Straßenverkehrsgesetzes (StVG) aufgrund der Zweiten EG-Führerschein-Richtlinie haben wir drei Führerscheinstellen überprüft. Es wurde festgestellt, daß die Umsetzung der rechtlichen Vorgaben des StVG und der Straßenverkehrszulassungsordnung (StVZO) insbesondere im Bereich der Fahrerlaubnisentziehung große Unterschiede aufwies. Dies hängt offenbar mit der **mangelnden Rechtsklarheit** der Straßenverkehrsvorschriften zusammen.

Über die Jahre ist eine **Fülle von Verwaltungsvorschriften** ergangen, die teilweise in Vergessenheit gerieten, aber nie außer Kraft gesetzt wurden. Den Mitarbeitern einer Führerscheinstelle war beispielsweise ein Erlaß aus dem Jahre 1974, der die Aufbewahrungsfristen für Akten über Fahrerlaubnisentziehungen regelt, überhaupt nicht bekannt.

Im einzelnen haben wir folgende Feststellungen getroffen:

– **Keine Gnade für Verkehrssünder?**

  Strafurteile, Bußgeldbescheide und Auszüge aus den zentralen Registern werden teilweise noch **Jahrzehnte** nach der Löschung im Bundeszentralregister und dem Verkehrszentralregister bei den Führerscheinstellen in Akten **aufbewahrt**.

  So fanden sich z.B. in einer Fahrerlaubnisakte Urteile nebst voller Begründung aus den Jahren 1965 und 1969, mit

denen Verkehrsverstöße geahndet wurden, obwohl nach dem im Oktober 1987 vom **Bundeszentralregister** ausgestellten Führungszeugnis diese Delikte dort nicht mehr gespeichert waren.

Eine andere Akte enthielt Vorgänge aus den Jahren 1957 und 1968 mit **sensiblen Daten** über den **Gesundheitszustand** des Betroffenen, dem 1968 die Fahrerlaubnis entzogen wurde mit der Möglichkeit, ab 1969 einen Antrag auf Wiedererteilung zu stellen. Im Jahre 1983 beantragte der Betroffene die Neuerteilung der Fahrerlaubnis. Der Antrag wurde von ihm jedoch 1984 zurückgezogen. Danach erfolgte kein weiterer Schriftwechsel.

Wir haben die zeitlich unbegrenzte Speicherung derartiger Sachverhalte nach Ablauf der Tilgungsfristen im Bundeszentralregister (BZR) und im Verkehrszentralregister (VZR) **beanstandet**, da nicht mehr zur Aufgabenerfüllung erforderliche personenbezogene Daten nach dem LDSG zu löschen sind.

Zur Begründung für die dauerhafte Speicherung von Straßenverkehrsvergehen wurde eine Bestimmung im Bundeszentralregistergesetz herangezogen. Danach kann eine frühere Entscheidung in einem Verfahren, das die Erteilung oder Entziehung einer Fahrerlaubnis zum Gegenstand hat, berücksichtigt werden, wenn die Verurteilung in das Bundeszentralregister einzutragen war. Die Frage, ob z.B. ein 20 Jahre zurückliegendes Vergehen im Straßenverkehr tatsächlich noch zu Lasten des Antragstellers berücksichtigt würde, wurde jedoch von den geprüften Stellen verneint. Die **Erforderlichkeit** einer längeren Datenspeicherung konnte mithin **nicht überzeugend begründet** werden.

Zu berücksichtigen ist hier überdies der **Resozialisierungsgedanke**, der verfassungsrechtliche Wurzeln hat und für den Bereich der Verkehrsdelikte nicht weniger bedeutsam als für das übrige Strafrecht ist.

– **Speicherung personenbezogener Daten ohne Aktenbeleg**

Zu kritisieren waren auch Datenspeicherungen in der Führerscheindatei. Hier wurden auch lange **nach Vernichtung** der entsprechenden **Aktenvorgänge** z.B. immer noch **Hinweise** darauf **gespeichert**, daß eine Fahrerlaubnis wegen Trunkenheit im Straßenverkehr entzogen worden war.

Nicht selten fanden sich Aufzeichnungen über Delikte aus den 60er Jahren. Auch dies wurde beanstandet, weil gerade bei ausschließlich elektronischer Datenspeicherung **jederzeit** die **Herkunft** der Daten und der Zweck ihrer Speicherung **feststellbar** sein müssen.

– **Sinnlose Datenspeicherung**

Bei einer Führerscheinstelle lag ein besonderes Beispiel an **sinnlosen Datenspeicherungen** vor. Dort hatte man über Jahre hinweg in einem freien Datenfeld ein **„E"** als Kürzel

entweder für die **Entziehung einer Fahrerlaubnis** oder die Erteilung eines **Ersatzführerscheines** gespeichert. Je nach Häufigkeit der Vorfälle konnte festgestellt werden, daß bis zu drei „E" bei Betroffenen vermerkt worden waren.

Die so gespeicherten Daten konnten nicht durch Akten belegt werden. Sie lassen nur noch **Vermutungen** zu, ob es sich dabei um Entziehungen oder Ersatzführerscheine gehandelt haben könnte. Solche Daten führen fast zwangsläufig zur Gefahr von **Fehlinterpretationen**. Da sie nicht mehr gedeutet werden können, sind sie für die verarbeitende Stelle nicht mehr verwendbar und damit auch nicht mehr erforderlich. Sie müssen gelöscht werden.

Wir haben überdies empfohlen, Inhalt und Umfang der Eingaben in **Freitextfelder** per **Dienstanweisung** festzulegen, damit sichergestellt werden kann, daß der Inhalt der Daten auch bei Bearbeiterwechsel nachvollziehbar bleibt.

– **Wie leicht man in Rechtfertigungszwang geraten kann**

Welche **Auswirkungen** eine **dauerhafte Speicherung** von Daten haben kann, hat der Fall eines Fahrerlaubnisinhabers gezeigt, der sich mit einer Eingabe an uns gewandt hatte. Fast zehn Jahre schlummerten seine Daten im Computer der Führerscheinstelle, bevor sie dann wirklich zu Schwierigkeiten führten.

Der **Verlust des Führerscheines** des Petenten brachte es an den Tag. Als dieser im Mai 1994 zu seiner Führerscheinstelle ging, um einen Ersatzführerschein zu beantragen, wurde ihm mitgeteilt, daß er gar keine Fahrerlaubnis besitze. Denn nach „Auskunft der automatisierten Datei" habe man ihm diese wegen des Verdachts einer Trunkenheitsfahrt im November 1984 abgenommen. Zur Untermauerung wurde ihm der Beschluß des Amtsgerichts vom 27.11.1984 über die vorläufige Entziehung vorgelegt.

Den Beteuerungen des Petenten, daß er deswegen **Mitte 1985 freigesprochen** und ihm damals am Ende der Hauptverhandlung sein Führerschein wieder ausgehändigt worden sei, wurde kein Glaube geschenkt. Er wurde lapidar **aufgefordert**, das **Urteil** über die Aufhebung der vorläufigen Entziehung **vorzulegen**, ansonsten bekäme er keinen Ersatzführerschein. Im Besitz des freisprechenden Urteils war der Petent jedoch nicht mehr. Als **Straftäter abgestempelt**, der fast zehn Jahre „ohne gültige Fahrerlaubnis" gefahren sei, wandte er sich empört an uns.

Bei unseren Nachprüfungen stellten wir fest, daß außer einer Karteikarte mit dem Beschluß der vorläufigen Entziehung und der Speicherung des Vermerks über die Sicherstellung in der automatisierten Datei **kein** weiteres **Aktenmaterial** vorhanden war.

Nach dem LDSG hätte die speichernde Behörde von sich aus tätig werden müssen, als von dem Petenten die Unrichtigkeit der Daten behauptet wurde. Wenn weder die Rich-

tigkeit noch die Unrichtigkeit gespeicherter Daten nachzuweisen ist, so müssen diese **gesperrt** und dürfen nicht gegen den Betroffenen verwandt werden. Somit hätte dem Petenten eine Ersatzfahrerlaubnis ausgestellt werden müssen.

Statt dessen wurde ihm aufgetragen, einen **Nachweis über** seinen **Freispruch** beizubringen. Selbst der Umstand, daß die vorläufige Entziehung schon fast zehn Jahre alt war und längst durch ein Urteil hätte bestätigt oder verworfen sein müssen, machte den Sachbearbeiter nicht nachdenklich.

Erst durch eine Ablichtung des Urteils, die wir bei der Staatsanwaltschaft erhielten, konnten wir die letzten Zweifel bei der Führerscheinstelle ausräumen. Die Daten wurden korrigiert und der Petent ist inzwischen im Besitz seines Ersatzführerscheines.

Bei dieser Gelegenheit stellten wir fest, daß das zuständige Amtsgericht es versäumt hatte, die Führerscheinstelle über den Freispruch in Kenntnis zu setzen. Dieser Umstand befreite die Führerscheinstelle aber nicht von der Pflicht, spätestens als der Petent einen Ersatzführerschein beantragte, selbständig Nachforschungen anzustellen und die Richtigkeit der gespeicherten Daten zu überprüfen.

– **Jeder Führerscheinentzug führt zu einer Meldung an die Polizei – „das haben wir immer so gemacht"**

Im Rahmen unserer Überprüfungen haben wir außerdem festgestellt, daß die Führerscheinstellen regelmäßig **Mitteilungen** über entzogene Fahrerlaubnisse an die **zuständigen Polizeiinspektionen** geben. In den Straßenverkehrsvorschriften fand sich für diese Datenübermittlungen keine Regelung. Auch auf die Vorschriften des Landesverwaltungsgesetzes konnten die Übermittlungen nicht gestützt werden, da eine im Einzelfall konkret bevorstehende Gefahr für die öffentliche Sicherheit nicht mehr vorlag. Nachforschungen bei der Polizei ergaben auch erhebliche **Zweifel an der Erforderlichkeit** der Datenübermittlung. Denn häufig sind die Zuständigkeitsbereiche der Polizeireviere so groß, daß die Polizeibeamten sich die Daten der von den Führerscheinstellen „gemeldeten" Personen nicht merken können. Die Mitteilungen werden z.B. in einem Polizeirevier zwar den Beamten jeweils zur Kenntnis gegeben, danach aber **abgeheftet** und in regelmäßigen Abständen **vernichtet**.

Für die praktische Polizeiarbeit, so wurde uns von der Polizei mitgeteilt, seien diese Mitteilungen nur in wenigen Einzelfällen hilfreich. Deshalb wurden diese Datenübermittlungen beanstandet.

– **INPOL-Fahndung nach entzogenen Führerscheinen**

Des weiteren stellten wir fest, daß Daten von Führerscheininhabern, deren Fahrerlaubnis z.B. wegen gesundheitlicher Bedenken oder charakterlicher Mängel entzogen worden war, in die **polizeiliche Fahndungsdatei** eingegeben wur-

den, wenn der betreffende Führerschein nicht abgeliefert wurde.

Das eigentliche verwaltungsrechtliche Zwangsverfahren wurde zwar eingeleitet, aber nicht weiter verfolgt. Das **Zwangsgeld**, so bekamen wir als Auskunft, werde nur **„pro forma"** angedroht, aber nicht festgesetzt, da die Beitreibung von Zwangsgeldern fast nie erfolgreich sei. Die Eingabe der Daten in die INPOL-Datei bringe für die Führerscheinstelle weniger Arbeit, verspreche aber mehr Erfolg.

Auf diese Weise werden entzogene Fahrerlaubnisse **bundesweit** zusammen mit Daten, die der **Fahndung** nach **Schwerverbrechern** dienen, gespeichert. So können sogar hochsensible Daten in das INPOL-System gelangen. In einem Fall wurde von der Führerscheinstelle im Ausschreibungsformular der Hinweis **„BTM-Konsument"** angekreuzt und demgemäß in der Fahndungsdatei gespeichert, obwohl dies mit der Suche nach einem Führerschein beim besten Willen nichts zu tun hatte. Rechtsgrundlagen für dieses Verfahren konnten uns nicht genannt werden.

Gründe der Praktikabilität vermögen eine Maßnahme wie die bundesweite Fahndungsausschreibung schon unter Verhältnismäßigkeitsgesichtspunkten nicht zu rechtfertigen. Wir haben auch dieses Verfahren beanstandet.

– **Altkartei und EDV**

Die Tatsache, daß eine Fahrerlaubnis erteilt worden ist, wird bei allen Führerscheinstellen in automatisierten Dateien gespeichert. Nur wenige Führerscheinstellen im Lande Schleswig-Holstein arbeiten noch mit manuellen Karteien.

Da jedoch bei der Umstellung von den Karteikarten auf die automatisierte Speicherung **massive Eingabefehler** durch ungeschulte Aushilfskräfte vorgekommen waren, wurden die Altkarteien, die zwar nicht mehr mit den automatisiert gespeicherten Daten übereinstimmten, zur gelegentlichen Fehlerkorrektur aufbewahrt. Diese **doppelte Datenhaltung** wurde von uns beanstandet. Die Führerscheinstellen wurden aufgefordert, innerhalb eines kurzen Zeitraumes die elektronisch gespeicherten Daten zu überprüfen und die manuellen Altkarteien zu vernichten.

Sie machen allerdings geltend, daß eine **Fehlerbereinigung** und anschließende Vernichtung der Altkarteien innerhalb eines halben Jahres aus personellen und finanziellen Gründen nicht möglich sei. Falsche Sparsamkeit in der Vergangenheit, nämlich der Einsatz mangelhaft geschulten Personals für die Datenerfassung, hat hier wie auch in anderen Fällen höhere Kosten zur Folge.

Fazit

Die Ergebnisse unserer Prüfungen wurden mit dem **Ministerium für Wirtschaft, Technik und Verkehr** erörtert. Es wurde **weitgehende Übereinstimmung** in der datenschutzrechtlichen Beurteilung erzielt. Bis zur Einführung der geplanten

Fahrerlaubnisverordnung im Zuge der Umsetzung der Zweiten EG-Führerschein-Richtlinie beabsichtigt das Ministerium, den Führerscheinstellen in einem Erlaß klare Vorgaben für die Datenverarbeitung in diesem Bereich zu geben.

Das Ergebnis der Prüfung zeigt auch, daß es dringend geboten ist, die geplante **Fahrerlaubnisverordnung** des Bundes präzise zu fassen, um sicherzustellen, daß wirklich nur solche Informationen gespeichert werden, die für die Verkehrsverwaltung erforderlich sind. Im Hinblick darauf, daß in den Verfahrensakten oft besonders sensible medizinisch-psychologische Gutachten, die auch intimste Details über Betroffene enthalten können, gespeichert werden, sind die Vorgaben so klar zu gestalten, daß sie auch durch die Führerscheinstellen vor Ort umgesetzt werden können.

Durch eine geprüfte Führerscheinstelle wurde demonstriert, daß es auch bei der derzeitigen Rechtslage anders geht und daß auch ohne langjährige und umfassende Datenspeicherungen erfolgreiche Verwaltungsarbeit geleistet werden kann. Sie zeichnete sich durch eine **Aktenhaltung** aus, die ausschließlich **aktuelle** und **zeitnahe Unterlagen** enthielt. Hier wurde schon seit Jahren praktiziert, was wir jetzt auch von den anderen Führerscheinstellen verlangt haben, nämlich nur die wirklich für das Verwaltungsverfahren erforderlichen personenbezogenen Daten zu verarbeiten und die Tilgungsfristen der Strafregister zu beachten. Derzeit wird in dieser Führerscheinstelle auch ein automatisiertes Verfahren eingeführt, welches es erleichtert, zu vernichtende Vorgänge herauszufinden und zeitnah auszusondern.

4.6.2 Was bei der Weitergabe von Führerscheinakten an medizinische Gutachter zu beachten ist

Vor Einverständniserklärungen für medizinisch-psychologische Eignungsuntersuchungen nach der Straßenverkehrs-Zulassungsordnung müssen Betroffene über die Verarbeitung ihrer personenbezogenen Daten aufklärt werden.

Die **Vordrucke** für die Erteilung des Einverständnisses eines Führerscheinbewerbers gegenüber der Führerscheinstelle zur Durchführung ärztlicher oder medizinisch-psychologischer Gutachten sind inhaltlich unterschiedlich und bei Anlegung datenschutzrechtlicher Maßstäbe **unzureichend**. In Gesprächen mit dem Ministerium für Wirtschaft, Technik und Verkehr haben wir Verbesserungen erreicht.

Die Betroffenen werden künftig außerdem gezielt darauf hingewiesen, daß sie **vor Übersendung** der Verwaltungsunterlagen an die Gutachterstelle das Recht haben, **Einsicht** in die für die Untersuchung für erforderlich gehaltenen Unterlagen zu nehmen. Darüber hinaus können sie gegenüber der Verkehrsbehörde auf ihrer Meinung nach sachfremde Angaben hinweisen. Dies ist von der Verkehrsbehörde schriftlich fest-

zuhalten. Damit sind drei Ziele erreicht: Zunächst wird der Betroffene **umfassend** über seine **Rechte aufgeklärt**. Er kann darüber hinaus Inhalt und Umfang der Informationen, die an die Gutachterstelle weitergeleitet werden, erkennen. Schließlich erhält er durch die Möglichkeit, **Einwendungen** gegen Inhalt und Umfang der zu übersendenden Verwaltungsvorgänge schriftlich bei der Verkehrsbehörde festhalten zu lassen, eine bessere Ausgangsposition in evtl. von ihm betriebenen Widerspruchs- und Klageverfahren.

4.7 Sozialwesen

4.7.1 Überprüfungsbogen „Wohn- und Wirtschaftsgemeinschaft" revidiert

Neugierige Fragen nach der Nutzung des Schlafzimmers wollen die Behörden in Schleswig-Holstein im Zusammenhang mit der Gewährung von Sozialhilfeleistungen künftig nicht mehr stellen.

Im letzten Tätigkeitsbericht (16. TB, S. 55) hatten wir über unzulässige Fragen in einem in Schleswig-Holstein gebräuchlichen Überprüfungsbogen zur „Wohn- und Wirtschaftsgemeinschaft/eheähnliche Gemeinschaft" berichtet und dargestellt, daß wir einen Teil der Fragen für unzulässig halten.

In diesem Zusammenhang hat das Bundesverfassungsgericht sogar ausdrücklich die Verpflichtung der Gerichte betont, Rechtsschutz zu gewähren, wenn es die Ämter „an dem gebotenen **Respekt vor der Intimssphäre**" des Bürgers fehlen lassen (BVerfG E 87, 234, 269). Die Annahme, es liege eine eheähnliche Gemeinschaft vor, setze nicht die behördliche Feststellung voraus, daß zwischen den Partnern geschlechtliche Beziehungen bestehen.

Angesichts dieser höchstrichterlichen Rechtsprechung haben wir gefordert, auf **Fragen** aus dem **Intimbereich** zu **verzichten** und sich auf die auch vom Bundesverfassungsgericht als Indizien für das Vorliegen einer eheähnlichen Gemeinschaft genannten Aspekte zu beschränken:

- Die Dauer des Zusammenlebens,
- die Versorgung von Kindern und Angehörigen im gemeinsamen Haushalt,
- die Befugnis, über Einkommen und Vermögensgegenstände des anderen zu verfügen.

Als nicht erforderlich und daher unzulässig haben wir das **Abfragen von privaten Verhaltensweisen**, die im Zweifel kaum überprüfbar und damit auch nicht justitiabel sind, bezeichnet. Im einzelnen handelt es sich dabei um Auskünfte darüber,

- wer die Räume pflegt, einkauft, kocht, bügelt, Geschirr und Wäsche wäscht und einsortiert,

– ob gemeinsam gegessen, ferngesehen, Zeitung gelesen oder ins Kino gegangen wird.

Die Erörterung, ob eine mehr oder weniger gemeinsame Lebensgestaltung vorliegt, kann in einer individuellen Einzelbefragung oder Beratung Sinn machen, erscheint jedoch untauglich für ein routinemäßiges Abfragen per Formular.

Unsere Bemühungen haben folgendes ergeben: Die Mehrzahl der Landkreise und kreisfreien Städte wird die **Fragebögen** entsprechend unseren Vorstellungen **überarbeiten** bzw. auf die formularmäßige Befragung gänzlich verzichten und nur noch eine auf den individuellen Einzelfall bezogene Datenerhebung vornehmen. Zwei Kreise wollen die künftige Verfahrensweise erst auf der nächsten Arbeitstagung der Wohngeldsachbearbeiter erörtern. Ein Kreis hat uns zwar mitgeteilt, er werde künftig nicht mehr nach der gemeinsamen Nutzung des Schlafzimmers fragen, jedoch gleichzeitig geltend gemacht, die Verwaltungsgerichte legten Wert auf Auskünfte, die für sich genommen „nichtssagend" erschienen. Angesichts der „Realität des Alltags" in den Sozialämtern stoße es auf Unverständnis, wenn es dem Antragsteller überlassen bleiben solle, inwieweit er Einblick in seine Privatsphäre geben wolle.

Wir werden uns durch weitere Nachprüfungen ein Bild verschaffen, ob durch eine neue Verfahrensweise tatsächlich die **Intimsphäre** von Antragstellern für den Wohngeldbezug **besser respektiert** wird.

4.7.2 Angaben zur Sozialhilfe auf Überweisungsträgern

Auch im Zahlungsverkehr mit den Banken ist das Sozialgeheimnis zu wahren. Auf Überweisungsträgern darf kein Hinweis auf Sozialhilfe erscheinen.

Bereits in der Vergangenheit hatten wir uns wiederholt mit der Frage zu beschäftigen, ob die Sozialleistungsträger auf ihren Überweisungen im Feld „Verwendungszweck" Angaben wie z.B.: „Sozialhilfe gemäß Bescheid vom ... AZ: ..." machen dürfen. In solch einem Fall wird das **Sozialgeheimnis verletzt**, weil die Bank ohne Not erfährt, daß der Kunde ein Sozialhilfeempfänger ist. Vielen Menschen war dies derart unangenehm, daß sie sich an uns gewandt oder vereinzelt sogar Gerichtsverfahren angestrengt haben, um diese Hinweise zu unterbinden. Auch wir haben stets darauf gedrungen, daß möglichst überhaupt kein entsprechender Hinweis auf dem Überweisungsträger erscheint.

Die Leistungsträger haben die Kennzeichnung ihrer Zahlungen deshalb für unverzichtbar gehalten, weil **Sozialleistungen nicht gepfändet** werden dürfen. Sei die Überweisung entsprechend gekennzeichnet, könne bereits die Bank überwiesene Beträge sofort für sich behalten, wenn ein Kunde seine Schulden nicht pünktlich zurückzahle, oder ein anderer Gläubiger das Geld pfänden. Dies sei jedoch dann ausgeschlossen, wenn die Zahlung schon der Bank gegenüber unmißverständlich als

„Sozialleistung" ausgewiesen werde. Unsere Auffassung wurde nunmehr vom **Bundesverwaltungsgericht** bestätigt. Das Gericht hält eine routinemäßige Offenbarung gegenüber einem Geldinstitut im Hinblick auf den genannten Pfändungsschutz nicht für erforderlich. Es sei allein Sache des Hilfeempfängers, sich für den Pfändungsschutz zu entscheiden und zu diesem Zweck der Offenbarung des Bezuges von Sozialleistungen zuzustimmen.

Die Hilfeempfänger sind also künftig darüber zu informieren, daß sie ihr Geldinstitut selbst (evtl. durch Vorlage des Bescheides) auf den Pfändungsschutz aufmerksam machen können. In anderen Bundesländern wird bereits seit längerer Zeit so verfahren, ohne daß Beschwerden bekannt geworden sind.

4.7.3 Sozialdatenschutz beim Publikumsverkehr

Der Schutz des Sozialgeheimnisses muß auch im Rahmen des behördlichen Publikumsverkehrs beachtet werden. Die Möglichkeit von Einzelgesprächen muß vorgesehen und den Bürgern auch tatsächlich angeboten werden.

Petenten teilten uns mit, daß es in der Sozialstation einer Stadt immer wieder zu gravierenden Verstößen gegen den Datenschutz komme. Es würden gleichzeitig **mehrere Personen im selben Raum** abgefertigt. Da es um die Bearbeitung von Sozialleistungsanträgen gehe, müßten die Besucher teilweise sehr **persönliche Angaben** zu ihren Einkommens-, Vermögens- und Wohnverhältnissen machen. Die Petenten empfanden es als äußerst unangenehm, daß Dritte ihre sensiblen personenbezogenen Daten zur Kenntnis nehmen konnten. Da die Offenbarung dieser Daten jedoch Voraussetzung für den Bezug von Leistungen war, sahen sie keine Möglichkeit, sich zur Wehr zu setzen.

Nachdem wir die betroffene Kommune darauf aufmerksam gemacht hatten, daß es sich bei der geschilderten Vorgehensweise um eine **eindeutige Verletzung** des **Sozialgeheimnisses** handele, teilte sie uns mit, die räumlichen und personellen Verhältnisse hätten vorübergehend keine andere Sachbehandlung zugelassen. Durch Personalabbau werde jedoch künftig jeder Mitarbeiterin bzw. jedem Mitarbeiter ein Büro für die Beratung von Besuchern zur Verfügung stehen.

Nach dem Sozialgesetzbuch haben die Sozialleistungsträger die **technischen** und **organisatorischen Maßnahmen** einschließlich der Dienstanweisungen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Sozialgesetzbuches zu gewährleisten. Zur Gewährleistung des **Sozialgeheimnisses** sind die Behörden verpflichtet, sicherzustellen, daß unbefugte Dritte keinen Zugang zu Sozialdaten haben. Dies bedeutet auch, daß zu gewährleisten ist, daß in diesem sensiblen Bereich eine **Einzelabfertigung** der betroffenen Bürger erfolgt.

Dies hat die Stadt für Zukunft zugesagt. Sie wurde von uns aufgefordert, jeden Besucher im Sozialzentrum auf die Möglichkeit der Einzelberatung hinzuweisen.

4.8 Gesundheitswesen

4.8.1 Chipkarten im Gesundheitswesen

Die neuen Krankenversicherungschips sind keineswegs fälschungssicher. Sollen auf Chipkarten auch medizinische Daten gespeichert werden, sind Sicherheitsvorkehrungen neuer Qualität notwendig.

Nimmt man die Häufigkeit, mit der in den vergangenen Monaten das Begriffspaar „Chipkarte" und „Gesundheit" in der Presse und in öffentlichen Diskussionen gemeinsam benutzt worden ist, als Maßstab, könnte man glauben, **Chipkarten** seien **die** neue **Heilmethode** und aus medizinischer Sicht vergleichbar mit der Erfindung des Penicillin. Industrie und Krankenkassen wollen uns glauben machen, ohne Chipkarte gehe im Gesundheitswesen gar nichts mehr, mit Chipkarte gehe alles besser.

Andere wiederum rücken diese kleinen Kärtchen mit dem goldfarbenen Prozessorchip in die Nähe eines hochtoxischen Stoffes, der genau das Gegenteil von dem bewirke, was als sein Nutzen dargestellt werde.

Bei all dieser **Euphorie** auf der einen und **Skepsis** auf der anderen Seite waren es einmal mehr die Datenschutzbeauftragten, die für eine **Versachlichung der Diskussion** sorgen mußten. Sie hatten also wie z.B. bei der Volkszählung, der Einführung der maschinenlesbaren Personalausweise, der gesetzlichen Regelung der Rasterfahndung oder der Diskussion um den großen Lauschangriff eine Aufgabe zu übernehmen, die eigentlich denjenigen obliegt, die neue technische Systeme „in die Welt setzen". Im Grunde geht es nämlich um drei einfache Fragen, auf die überzeugende und ehrliche Antworten gegeben werden müssen:

- Was wird von wem mit dem technischen System bezweckt?
- Wie funktioniert es?
- Wie werden welche „schädlichen Nebenwirkungen" verhindert?

Als ein neues Musterbeispiel dafür, wie man es nicht machen sollte, stellt sich die Einführung der Krankenversicherungskarte dar. Versucht man in diesem Zusammenhang auf die o.a. Fragen eine befriedigende Antwort zu finden, werden die Defizite deutlich:

Frage 1: Was wird von wem mit dem Ersatz des papierenen Krankenscheins durch die Krankenversicherungschipkarte bezweckt?

Da die Krankenversicherungskarte durch das **Gesundheitsreformgesetz von 1988** eingeführt worden ist, dürfte man vermuten, daß wichtige öffentliche Belange die Umstellung gebieten und daß die Zweckbestimmung entsprechend den Vorgaben des Volkszählungsurteils von 1983 normenklar dem Gesetz zu entnehmen wäre. Ein Blick in den entsprechenden Teil des Sozialgesetzbuches ist allerdings ernüchternd. Im wesentlichen wird nur festgestellt:

- Die Krankenkasse stellt für jeden Versicherten eine Krankenversicherungskarte aus, die den Krankenschein ersetzt.
- Sie darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der ärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden.
- Sie enthält folgende Angaben: Ausstellende Krankenkasse, Namen des Versicherten, Geburtsdatum, Anschrift, Krankenversicherungsnummer, Versichertenstatus, Beginn des Versicherungsschutzes, Gültigkeitsablauf der Karte.
- Die Spitzenverbände der Krankenkassen und der kassenärztlichen Bundesvereinigungen vereinbaren das Nähere über die bundesweite Einführung und Gestaltung der Krankenversicherungskarte.

Kein Wort also zur **Benutzungspflicht** und zu den **konkreten Auswirkungen** für die Betroffenen. Die Regelung enthält auch keinen Hinweis darauf, daß es sich bei der Krankenversicherungskarte um eine Prozessorchipkarte handeln sollte. Das Gesetz bleibt diese Antworten schuldig. Und was sagten die Protagonisten? Bis heute gibt es in den Publikationen der Krankenkassen zwei ganz unterschiedliche Hinweise auf den Zweck der Maßnahme:

a) Es werden **Kosteneinsparungen angestrebt.**
Wo, in welcher Höhe und wann sich aber die Einführungskosten von ca. 500 Millionen DM für die 72 Millionen Karten und die 130.000 Lesegeräte amortisieren sollen, bleibt bislang im dunkeln.

b) Es handelt sich um die Vorstufe zu einem ganz **neuen Abrechnungsverfahren** in dem Dreieck „Patient – Arzt – Krankenkasse". Wie aber das „Verfahren" aussehen soll, erweist sich als ein streng gehütetes Geheimnis.

Frage 2: Wie funktioniert die Chipkarte, was passiert bei ihrer Benutzung?

Die **Entscheidung** für Mikroprozessortechnologie als Datenspeicher ist ganz allein von den **Krankenkassen** getroffen worden. Fragen wie: „Warum so und nicht anders?" und „Wie funktioniert der Chip?" hätten also von ihnen beantwortet werden müssen. Es ist zwar viel geschrieben worden über zertifizierte Lesegeräte, Prüfziffern und dergleichen, aber man blieb recht allgemein. Auf die Frage, warum z. B. der Datenspeicher größer ist als für die zulässigen Daten erforderlich, gab es keine überzeugende Antwort.

Eine weitere Ungereimtheit: In einer Publikation wird erläutert, daß Änderungen der Anschrift nur durch die betreffende Krankenkasse in dem Chip vorgenommen werden könnten, bei anderen Änderungen würde eine neue Krankenversicherungskarte erstellt. Hieraus wurde allgemein geschlossen, die anderen in dem Chip gespeicherten Daten seien unveränderbar. Um so größer war das Erstaunen, als einige Wochen nach Einführung der Karten Geräte frei käuflich waren, mit denen alle **Speicherungen verändert** werden konnten. Wir haben uns in unserem PC-Labor von der „Machbarkeit" selbst überzeugt. Auch das zur Plausibilitätsprüfung benutzte Prüfziffernverfahren erwies sich nicht als „geheim". Der hochgelobte Prozessorchip ist also in dieser Form genauso manipulierbar wie der Magnetstreifen auf den Scheckkarten.

Frage 3: Wie werden welche „schädlichen Nebenwirkungen" verhindert?

Von den Krankenkassen wurden die Krankenversicherungskarten zunächst als „nebenwirkungsfrei" deklariert. Erst kritisches Hinterfragen brachte **Risiken** zutage wie z. B.: Möglichkeit des „Ärzteshopping", widerrechtliche Benutzung über lange Zeiträume, fehlende Identitätsprüfungen und dergleichen. Die Krankenkassen reagierten gelassen. All dies führe zwar zu finanziellen Schäden für die Kassen, diese seien aber einkalkuliert, die Versicherten hätten keine Nachteile zu befürchten.

Alles in allem also eine **wenig überzeugende Verfahrensweise**. Gleichwohl haben die Datenschutzbeauftragten keine wirklichen Gründe für Beanstandungen gefunden und „gute Miene zum bösen Spiel" gemacht. Der Grund lag darin, daß nach datenschutzrechtlichen Maßstäben in der Tat keine Beeinträchtigungen schutzwürdiger Belange der Versicherten zu erwarten sind. Das gespeicherte **Datenprofil** ist einfach zu **trivial**, als daß ein wie auch immer gearteter Schaden für die Betroffenen entstehen könnte.

Um so größer muß aber die Wachsamkeit der Datenschutzbeauftragten sein, wenn die Krankenkassen beginnen, die Krankenversicherungskarte zu einer **Gesundheitschipkarte** „aufzubohren". Ansätze hierzu gibt es in Hülle und Fülle. In dem Moment nämlich, in dem neben den Grunddaten auch medizinische Informationen gespeichert werden sollen, erhält die Chipkarte eine **völlig neue Qualität**. Neben vielen ungelösten Problemen in bezug auf die Gewährleistung der Richtigkeit und der richtigen Interpretation der medizinischen Daten steigen die **sicherheitstechnischen Anforderungen** in einer Größenordnung von Quantensprüngen.

Selbst bei einer ausschließlich freiwilligen Benutzung solcher Karten durch die Patienten bzw. Versicherten sind nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder **folgende Bedingungen** zu erfüllen:

- Die Ausgabe der Gesundheitskarten und die damit verbundenen Speicherungen von Gesundheitsdaten bedarf der

schriftlichen Einwilligung der Betroffenen. Sie sind umfassend über Zweck, Inhalt und Verwendung der angebotenen Karten zu informieren.

- Die freiwillig benutzten **Gesundheitskarten** dürfen nicht – etwa durch Integration auf einem Chip – die **Krankenversicherungskarten** nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karten sind technisch so zu gestalten, daß für die **einzelnen Nutzungsarten** nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Die **Betroffenen** müssen von Fall zu Fall und ohne Benachteiligung – z.B. gegenüber den Ärzten, der Krankenkasse oder sonstigen Versicherungen – **entscheiden** können, ob sie die Gesundheitskarte zum Lesen der Gesundheitsdaten vorlegen oder ob sie ggf. den Zugriff auf bestimmte Daten beschränken.
- Sie müssen ferner frei entscheiden können, **wer welche Daten** in den Datenbestand übernehmen darf.
- Der **Umfang der Daten**, die gelesen oder übernommen werden, darf außerdem nicht über den für die gesetzliche Aufgabenstellung bzw. den Vertragszweck erforderlichen Umfang hinausgehen. Die Kartenaussteller müssen sicherstellen, daß die Betroffenen **jederzeit** vom Inhalt der Gesundheitskarte unentgeltlich **Kenntnis** nehmen können.
- Die Betroffenen müssen jederzeit **Änderungen** und **Löschungen** der gespeicherten Daten veranlassen können.

Zu den allgemeinen technischen Aspekten von Prozessorchipkarten vgl. Tz. 7.2.

4.8.2 Prüfung in einer psychiatrischen Klinik

Die Kontrolle in einer psychiatrischen Klinik hat ergeben, daß dort Datenschutzrecht verletzt worden ist. Es waren z.B. noch Behandlungsakten aus dem letzten Jahrhundert vorhanden.

Im Berichtsjahr konnte die Überprüfung der Verarbeitung personenbezogener Daten in einer psychiatrischen Klinik abgeschlossen werden. Die **Patienten** der Klinik halten sich dort entweder **freiwillig** aufgrund eines Behandlungsvertrages auf oder sind **zwangsweise** aufgrund der entsprechenden gesetzlichen Vorschriften (etwa nach dem Strafgesetzbuch oder dem Gesetz über psychisch Kranke) untergebracht. Letzteres beinhaltet gleichzeitig die zwangsweise Behandlung der Betroffenen.

Alle in einer solchen Fachklinik verarbeiteten Daten der Patienten unterliegen der **ärztlichen Schweigepflicht**. Die unbefugte Weitergabe dieser Daten – und dies gilt auch bezüglich der zwangsweise untergebrachten Patienten – ist nach dem Strafgesetzbuch strafbar. Datenübermittlungen sind also nur

aufgrund von Rechtsvorschriften oder mit dem Einverständnis der Betroffenen zulässig.

Die **ärztliche Schweigepflicht** ist jedoch nicht nur bei Übermittlungen nach „draußen" zu beachten, sondern auch **innerhalb der Klinik**. Dies kann bei neuen Methoden wie der Arbeit „im Team" zu Problemen führen. Die Arbeit im Team, also der Ärzte, der Psychologen, der Therapeuten, des Pflegepersonals, des für die Station zuständigen Sozialarbeiters sowie der Stationshilfen, sei Voraussetzung für eine sinnvolle Arbeit im psychiatrischen Bereich, so wurde seitens der Klinik betont. Vorgetragen wurde in diesem Zusammenhang auch die Ansicht, Teamarbeit bedinge, wenn sie denn effektiv sein solle, daß auch alle **nichtärztlichen Mitarbeiter** Zugriff auf alle Informationen der Krankengeschichte haben.

Im einzelnen haben wir folgende Feststellungen und Wertungen getroffen:

Löschung von Krankenakten

Bisher ist keine Löschung oder Sperrung von Patientendaten erfolgt. Die Klinik bewahrt **Krankengeschichten seit 1820** auf, allerdings fehlen dazwischen Jahrgänge, so z.B. aus der NS-Zeit. Konkrete Überlegungen zur Löschung von Daten wurden bisher nicht angestellt. Vernichtet wurden nur wenige für den kurzfristigen Gebrauch bestimmte Unterlagen.

Spezielle Rechtsvorschriften über die **Löschung von Patientendaten** gibt es in Schleswig-Holstein nicht. Die **ärztliche Berufsordnung** trifft lediglich eine Regelung über die Mindestaufbewahrungszeit von zehn Jahren. Die **Röntgenverordnung** sieht vor, daß Aufzeichnungen über die Untersuchung zehn Jahre, über die Behandlung 30 Jahre nach Abschluß der letzten Untersuchung oder Behandlung mit Röntgenstrahlen aufzubewahren sind.

Im übrigen sind also die allgemeinen Vorschriften des Landesdatenschutzgesetzes anzuwenden. Die Daten sind demnach zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung **nicht mehr erforderlich** ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Die Speicherungsdauer ärztlicher Daten hat sich also danach zu richten, wie lange sie für **Behandlungszwecke** benötigt werden. Nach Abrechnung der Behandlung sind die Unterlagen zunächst zehn Jahre entsprechend den Regelungen der ärztlichen Berufsordnung aufzubewahren. Über diese zehn Jahre hinaus muß weiter aufbewahrt werden, wenn es nach ärztlicher Erfahrung **im Einzelfall** geboten ist. Dabei ist nach unserer Auffassung zu berücksichtigen, daß gerade Daten über eine psychiatrische Behandlung in besonderem Maße sensibel sind. In einigen Bundesländern hat der Gesetzgeber weitgehend die Regelungen der Berufsordnung übernommen. Aus alledem ergibt sich, daß die Krankengeschichten im **Regelfall nach 10 Jahren** zu vernichten sind, sofern nicht im Einzelfall

eine besondere Entscheidung mit besonderer Begründung getroffen wird.

Tritt an die Stelle der Löschung die **Sperrung**, etwa weil schutzwürdige Interessen der Betroffenen der Löschung entgegenstehen, dann müssen die Unterlagen aber **gesondert aufbewahrt** oder **besonders gekennzeichnet** werden. Sie dürfen dann ohne Einwilligung der Betroffenen nur noch verwendet werden, wenn eine Rechtsvorschrift dies ausdrücklich zuläßt oder wenn die Verarbeitung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder von Dritten liegenden Gründen unerläßlich ist. Die Gründe für die ausnahmsweise Nutzung sind zu dokumentieren.

Diese **Bedingungen** waren in der Klinik **nicht eingehalten**, so daß wir die unterschiedslose Speicherung der Behandlungsakten über die Dauer von mehr als 10 Jahren beanstandet haben.

Bei einer zwangsweisen Unterbringung wird die Klinik nicht aufgrund eines Vertrages tätig, sondern aufgrund gesetzlicher Vorschriften. Spezielle Aufbewahrungsregelungen kennen aber auch die Spezialgesetze nicht. Die Aufbewahrung der Akten darf auch in diesen Fällen nur solange erfolgen, wie sie zur Aufgabenerfüllung der Fachklinik notwendig ist.

Datenschutz auf den Stationen

Die Prüfung auf den Stationen hat ergeben, daß dort vielfach **Sammlungen von Duplikaten** von Arztbriefen bestehen. Dieses ist aus datenschutzrechtlicher Sicht nur zu akzeptieren, wenn es sich um eine Aufbewahrung für einen vorübergehenden Zeitraum nach Abschluß der Behandlung handelt.

Es hat sich überdies gezeigt, daß auf den Stationen teilweise Unklarheit über die Vernichtung von Unterlagen herrscht. Es mußte beanstandet werden, daß Schriftstücke mit Daten, die dem Patientengeheimnis unterliegen wie Entwürfe, Notizen usw. **nicht ordnungsgemäß vernichtet** werden.

Sozialdienst

Die Klinik hat einen umfangreichen Sozialdienst aufgebaut, der in vielfältiger Form tätig wird. Die Mitarbeiter nehmen an den **Abteilungsvisiten** und **Teamgesprächen** teil und werden entweder von den Patienten selbst um Regelung ihrer Angelegenheiten gebeten oder von den Ärzten bzw. dem Pflegepersonal auf Probleme aufmerksam gemacht. So stellt der Sozialdienst z.B. Rentenanträge und Kostenübernahmeanträge an das Sozialamt und führt sonstigen Schriftwechsel für den Patienten mit Stellen von „außen".

So positiv diese Tätigkeit des Sozialdienstes auch sein mag, so ist gleichwohl die Frage nach der Rechtsgrundlage zu stellen, aufgrund derer ihm Patientendaten übermittelt werden

und er selbst Informationen über die Betroffenen nach „außen" weitergibt. Eine **spezielle gesetzliche Grundlage** für seine Tätigkeit **existiert nicht**. Nach dem Selbstverständnis des Sozialdienstes ist seine Tätigkeit **„Behandlung"**. Dies wird auch vom Ärztlichen Direktor so gesehen, weil dem Patienten nicht nur Sorgen abgenommen würden, die den medizinischen Erfolg beeinträchtigen könnten, sondern weil für einen weiteren positiven Verlauf des Heilungsprozesses auch bestimmte Startvoraussetzungen nach der Entlassung gegeben sein müßten, um in vielen Fällen einen sofortigen Rückfall zu verhindern.

Unproblematisch ist das Handeln des Sozialdienstes, wenn es mit dem **Einverständnis** des geschäftsfähigen, voll unterrichteten Patienten oder dessen Betreuer geschieht. Liegt dieses vor, so sollte es auch dokumentiert werden. Eine Besonderheit der Fachklinik besteht jedoch gerade darin, daß viele der dort versorgten Menschen zu einer rechtswirksamen Einwilligung nicht in der Lage sind. Entgegen der Auffassung der Klinik läßt sich die Tätigkeit des Sozialdienstes nicht unter den herkömmlichen Behandlungsbegriff subsumieren, weil darunter zunächst nur die rein ärztliche Versorgung verstanden wird. Selbst die Einbeziehung der ärztlichen Mitarbeiter hat immer unter direkter Verantwortung und Leitung des Arztes zu erfolgen. Davon kann jedoch bei dem selbständig organisierten und handelnden Sozialdienst nicht ausgegangen werden.

Es bleibt also festzustellen, daß dem Sozialdienst personenbezogene Informationen in erheblichem Umfang ohne Rechtsgrundlage offenbart worden sind. Dies mußten wir förmlich **beanstanden**. Der Gesetzgeber ist hier aufgefordert, auf Landesebene eine gesetzliche Grundlage zu schaffen.

Automatisierte Verarbeitung von Patientendaten

Die Überprüfung der automatisierten Datenverarbeitung der Fachklinik führte zur Feststellung von Mängeln und entsprechend zu folgenden Vorschlägen zur Verbesserung des Datenschutzes:

- **EDV-Dienstanweisung**

  In Form einer EDV-Dienstanweisung sollten allgemeine Vorgaben und Verfahrensregelungen für die Entwicklung und Auswahl von Hard- und Softwarekomponenten, ihren Text, deren Freigabe und Dokumentation definiert werden. Diese Dienstanweisung sollte für alle Bereiche der Fachklinik Gültigkeit haben, also für den ärztlichen, den Pflegebereich und die Verwaltung gleichermaßen verbindlich sein.

- **Datensicherungsregelungen**

  In Anbetracht der Tatsache, daß nahezu alle verarbeiteten personenbezogenen Daten einem besonderen Berufs- bzw. Amtsgeheimnis unterliegen, bedarf es konkreter Datensi-

cherungsregelungen für die automatisierten und die konventionellen Verfahrensabläufe, z.B. auch für die Verwaltung von Krankenakten und elektronischen Datenträgern.

– **Dateibeschreibungen**

Es sollten kurzfristig authentische Dateibeschreibungen und ein formgerechtes Geräteverzeichnis für alle EDV-Geräte, mit denen personenbezogene Daten verarbeitet werden (einschließlich der medizinischen Geräte) erstellt werden.

– **Sicherheitskonzepte**

Für neu entwickelte automatisierte Verfahren sollten Sicherheitskonzepte definiert werden, bevor die Verfahren zum Einsatz freigegeben werden.

– **Befugnisregelungen**

Es sollte eindeutig festgelegt werden, wer die Befugnis hat, automatisierte Verfahren bzw. Hardware- und Software-Komponenten zum Einsatz freizugeben (ggf. getrennt für den Verwaltungs-, den medizinisch-klinischen und den Pflegebereich). Die Benutzung nicht freigegebener Hard- und Software sollte ausdrücklich untersagt sein.

– **Soll-Ist-Vergleich**

Es sollte gewährleistet werden, daß die tatsächliche Nutzung automatisierter Verfahren regelmäßig durch die Führungsebene der Fachklinik gegen die Vorgaben (Soll-Ist-Vergleich) abgeglichen wird. Dies kann auch durch besonders beauftragte Mitarbeiter geschehen. Eine entsprechende Schulung der Führungskräfte, die das Erkennen von Schwachstellen in den Vorgaben und Abweichungen von ihnen ermöglicht, erscheint deshalb unverzichtbar. Wegen der „Sensibilität" der verarbeiteten Daten sollten revisionsfreie Räume nicht toleriert werden.

– **Verfahrensdokumentation**

Die Dokumentation der automatisierten Verfahren sollte so ausgestaltet sein, daß sie für Dritte nachvollziehbar ist. Dies gilt besonders für den medizinisch-klinischen Bereich. Bei Software, an der nur Nutzungsrechte bestehen, kann zwar auf die Dokumentation des Quellcodes, nicht aber auf die lückenlose Dokumentation der Abläufe und Inhalte der einzelnen Programm- und Verfahrensversionen und der Gründe für Änderungen verzichtet werden.

– **Befugnisdefinition**

Die Befugnisse und Verantwortungsbereiche der Systembetreuer aus der Direktionsstelle „DV-Organisation", aus den zuständigen Abteilungen sowie dem Pflegebereich sollten

eindeutig definiert werden. Dies gilt insbesondere auch für die Abgrenzung der Zuständigkeiten (welche Befugnisse hat z.B. der Systembetreuer der Verwaltung bezüglich der automatisierten Verfahren im medizinisch-klinischen Bereich?). Weiterhin bedarf es einer effektiven Vertretungsregelung. Wichtige Arbeiten auf Betriebssystemebene sollten nach dem Vier-Augen-Prinzip überwacht und hinreichend dokumentiert werden.

– **Rechte externer Hilfskräfte**

Die Befugnisse von Mitarbeitern der Systemhäuser sollten ebenfalls inhaltlich für das gesamte Klinikum geregelt werden. Ein Zugriff auf „echte" Daten scheidet grundsätzlich aus.

– **Paßwortvergabe**

Die Paßwortvergabe sollte in der Weise geregelt werden, daß die Paßworte von dem jeweiligen Benutzer selbst vergeben werden und nur ihm selbst bekannt sind. Paßwortänderungen sollten den Mitarbeitern jederzeit möglich sein.

– **Zugriffsbeschränkungen**

Die Zugriffsbefugnisse auf Datenbestände sollten geregelt und dokumentiert werden. Programmtests mit „echten" personenbezogenen Daten sind nicht zulässig.

– **Löschfristen**

Für alle personenbezogenen Datenbestände außerhalb der Krankenakten und der Abrechnungsdateien der Krankenhausverwaltung sollten möglichst kurze Löschungsfristen festgelegt werden. Dies gilt insbesondere auch für die Textdateien.

– **Schulungsprogramm**

Für die Schulung des mit automatisierten Verfahren befaßten Personals (insbesondere medizinisch-klinischen Bereich und für Führungskräfte) sollte eine Konzeption erarbeitet werden. Mitarbeitern sollte erst dann Verantwortung für die Steuerung und Überwachung automatisierter Abläufe übertragen werden, wenn sie entsprechend ausgebildet sind.

Reaktion der Fachklinik

– **Aufbewahrung der Krankengeschichten**

Zu der von uns kritisierten unbegrenzten Aufbewahrung von Krankenakten hat die Fachklinik angemerkt, daß

psychiatrische Krankengeschichten einen besonderen Stellenwert haben. Anders als in den übrigen Teilgebieten der Medizin seien in der Psychiatrie Angaben zur Vorgeschichte, zur Anamnese und zur Behandlung außerordentlich wichtig. Diese Angaben seien es nach Aussage der Klinik vielfach, die nach Jahrzehnten die Diagnose und damit die Therapie eines Wiederaufgenommenen ermöglichten.

Die Klinik wird künftig in den Behandlungsvertrag einen Passus aufnehmen, der die Patienten darüber aufklärt, daß die Daten in der Krankengeschichte grundsätzlich zehn Jahre gespeichert werden und danach eine Einzelfallprüfung erfolgt, ob eine weitere Aufbewahrung der Akte gerechtfertigt oder nötig ist.

– **Verfahren bei Arztbriefen**

Die Klinik bereitet eine Dienstanweisung vor, die das Verfahren bei der Einholung von Einverständniserklärungen der Patienten zur Weitergabe von Arztbriefen regelt.

– **Sozialdienst**

Nach Auffassung der Fachklinik wird der Sozialdienst im Rahmen der Behandlung des Patienten tätig.

Der Umgang mit Daten, die der ärztlichen Schweigepflicht unterliegen, wird nach Aussage der Fachklinik künftig wie folgt geregelt: Im Rahmen des Behandlungsprozesses werden an den Sozialdienst und andere an der Behandlung beteiligte Berufsgruppen grundsätzlich nur noch die im Einzelfall erforderlichen Daten weitergegeben.

– **Pflegedirektion**

Die Klinik hält nach wie vor eine umfassende Einsichtnahme des Pflegepersonals in die Patientenakte zur Erfüllung des Behandlungsauftrages der Fachklinik für notwendig.

– **Technische und organisatorische Maßnahmen zur Datensicherheit**

Unsere Verbesserungshinweise für die automatisierte Verarbeitung von Patientendaten sollen umgesetzt werden.

– **Dateibeschreibungen**

Die Fachklinik wird die Dateibeschreibungen vervollständigen und zum Dateienregister melden.

4.8.3 Prüfung einer Suchtberatungsstelle

Wenn Bürger freiwillig das Beratungsangebot einer staatlichen Stelle annehmen, so dürfen die im Laufe der Beratung von ihnen offenbarten Daten nicht ohne ihr ausdrückliches Einverständnis zu anderen Zwecken genutzt, gespeichert oder gar an Dritte weitergegeben werden.

Bei der Prüfung der Suchtberatungsstelle in einem Kreisgesundheitsamt stellten wir eine **unzureichende Abschottung** der Vorgänge des Suchtberaters gegenüber anderen Akten fest:

- Die Personalien der Beratenen wurden in die allgemeine Kartei des Sozialpsychiatrischen Dienstes aufgenommen.
- Komplette Vorgänge aus der Suchtberatung wurden zu anderen Akten des Sozialpsychiatrischen Dienstes genommen, ohne daß ein Einverständnis der Betroffenen erkennbar war.
- Generell mußten wir die Aufbewahrung der Beratungsakten kritisieren, da sie zusammen mit den übrigen Akten gelagert wurden.

Nach dem Strafgesetzbuch darf der Suchtberater als staatlich anerkannter Sozialpädagoge Privatgeheimnisse, die ihm im Laufe einer Beratung bekannt werden, nicht unbefugt offenbaren. Als **„offenbart"** gilt ein Geheimnis bereits dann, wenn es auf irgendeine dem Verpflichteten zurechenbare Weise einem anderen zur Kenntnis gelangt. Bei Schriftstücken genügt bereits das Schaffen der tatsächlichen Möglichkeit der Kenntnisnahme durch andere. So hat die Rechtsprechung es z.B. für unzulässig erklärt, daß der Berufspsychologe einer kommunalen Suchtberatungsstelle für Telefonate mit Betreuten die dienstliche Telefonanlage benutzte, weil diese über eine automatische Erfassung der angerufenen Telefonnummer verfügte und so nachvollziehbar war, mit wem er telefoniert hatte.

Als entscheidend haben wir hier angesehen, daß der Suchtberater seinen Probanden absolute Vertraulichkeit zusichert. Dies bedeutet, den Betreuten wird versprochen, daß tatsächlich nur er und sonst niemand von der Beratung an sich oder gar von Gesprächsinhalten erfährt. Die ausdrückliche **Zusicherung der Vertraulichkeit** ist für die Betroffenen gewissermaßen **Geschäftsgrundlage** für die Annahme des Beratungsangebotes. Soweit andere Personen auch nur die faktische Möglichkeit eines Zugriffs auf die Akten des Suchtberaters haben, ist die Wahrung dieser Verschwiegenheitspflicht nicht gewährleistet.

Als **Konsequenzen** haben wir **gefordert**:

- Entfernung der Unterlagen über Probanden des Suchtberaters aus der allgemeinen Datei des Sozialpsychiatrischen Dienstes,
- gesonderte Aufbewahrung der Suchtberatungsakten,
- zusätzliche Trennung der Aktenteile, die einem Beschlagnahmeverbot unterliegen.

Das Kreisgesundheitsamt hat erklärt, diese Maßnahmen durchführen zu wollen.

4.9 Kultusbereich

4.9.1 Aus dem Schulalltag

4.9.1.1 Der Umgang mit Entschuldigungsschreiben

Entschuldigungen von Schülerinnen und Schülern wegen des Fernbleibens vom Unterricht dürfen nicht zusammen mit dem Klassenbuch verwahrt werden. Es ist sicherzustellen, daß eine Einsichtnahme in Entschuldigungen durch Mitschüler und andere Unbefugte nicht möglich ist. Dies schließt es aus, Schüler mit der Entgegennahme von Entschuldigungen zu beauftragen.

In einer Berufsschule wurden für jede Klasse Stehordner als Klassenbücher verwendet. Hinter den Klassenbuchvordrucken wurden gesondert die Entschuldigungen, mit denen Eltern bzw. volljährige Schüler Unterrichtsversäumnisse rechtfertigten, abgeheftet. Aus den **Entschuldigungen** wegen krankheitsbedingten Fehlens waren häufig auch die **Krankheitsursachen** ersichtlich.

Der Schulleiter machte geltend, daß der Ordner nur den in der Klasse tätigen Lehrkräften zugänglich sei. Eine Einsichtnahme durch Schülerinnen oder Schüler schloß er zunächst kategorisch aus. Unmittelbar nach dieser Äußerung stellte sich das Gegenteil heraus. Im Aufzug trafen wir noch während unserer Prüfung einen Schüler mit einem Klassenbuchordner in der Hand an, der interessiert in den Entschuldigungen blätterte.

Wir haben die Abheftung von Entschuldigungen im Klassenbuch beanstandet und die Schulleitung aufgefordert sicherzustellen, daß Entschuldigungsschreiben für Unbefugte unzugänglich im Bereich der Schulverwaltung aufbewahrt werden.

In einem anderen Fall wurde uns bekannt, daß in einer Schulklasse die **Entschuldigungen** von einer **Mitschülerin entgegengenommen** und die Tatsache des entschuldigten Fehlens in das Klassenbuch eingetragen wurde. Nach der Stellungnahme der Schule diente diese Maßnahme der Förderung der Schülerpersönlichkeit und zur Erziehung der Schülerinnen und Schüler zur Verantwortung und Selbständigkeit.

Auf unseren Hinweis wurde diese Praxis eingestellt.

4.9.1.2 Wenn Schüler „Mist bauen"

Das Schulgesetz läßt die Übermittlung von Schülerdaten an private Stellen und Einzelpersonen nur mit Einwilligung der Betroffenen zu. Das gilt auch, wenn Schüler im Verdacht stehen, Dritten einen Schaden zugefügt zu haben.

Zwei Schüler rangelten auf dem Schulhof und beschädigten dabei ein dort parkendes Kraftfahrzeug. Der **Anwalt des Geschädigten** forderte die Schule auf, Geburtsdaten und Anschriften der ihm namentlich bekannten Schädiger mitzuteilen, weil er sie zur Rechtsverfolgung benötigte.

Das Schulgesetz läßt eine Datenübermittlung an Private **nur mit Einwilligung** der betroffenen Schüler oder ggf. ihrer Eltern zu. Diese Festlegung ist abschließend, da das Schulgesetz als bereichsspezifische Vorschrift Vorrang vor dem allgemeinen Datenschutzrecht hat. Ohne Einwilligung der Betroffenen darf die Schule dem Anwalt die geforderten Angaben nicht machen.

Ein „ähnlicher Fall" hatte jedoch andere Konsequenzen. Ein Schüler hatte einen anderen verletzt. Die Eltern des Verletzten begehrten Auskunft über die Identität des vermutlichen Schädigers. Auch hier wäre eine Auskunft an die Eltern nur mit Einwilligung des Betroffenen zulässig gewesen. Jedoch bestand in diesem Fall daneben ein Anspruch des geschädigten Schülers bzw. seiner Eltern auf Einsicht in das Unfallprotokoll. Auf diese Weise konnte die Identität des Beteiligten ermittelt werden. Die Einsichtnahme wäre nur dann zu versagen gewesen, wenn der Schutz Dritter dies geboten hätte. Die in jedem Einzelfall notwendige **Abwägung** zwischen Informationsinteresse des geschädigten Schülers und Schutzinteresse eines Schädigers dürfte dabei im Regelfall jedoch nicht zum Nachteil des Geschädigten ausgehen.

4.9.1.3 Verhaltensauffälligkeiten von Schülern

Wenn Verhaltensdaten von Schülern per Formblatt erhoben und in der Schule zentral gespeichert werden, entstehen Datensammlungen, die besonders gesichert werden müssen.

Eine Berufliche Schule erfaßte **Verhaltensauffälligkeiten** von zumeist volljährigen Berufsschülern wie

- Zuspätkommen zum Unterricht,
- Verlassen des Klassenraumes während des Unterrichtes,
- Fehlen in den Folgestunden nach Klausuren,
- Verdacht auf gezieltes Fehlen freitags und montags, vor und nach Klausurtagen,

monatsweise auf einem einheitlichen Vordruck. In ihrer Stellungnahme teilte die Schule mit, daß mit der systematischen Erfassung von verhaltensauffälligen Schülerinnen und Schülern mit Hilfe des Vordruckes eine **Grundlage für Beratungsgespräche** geschaffen werden solle, damit die Bildungs- und Erziehungsziele des Schulgesetzes erfüllt werden könnten. Der Erhebungsbogen diene dazu, konkrete Auffälligkeiten in einem Beratungsgespräch auch thematisieren zu können.

Unsere Nachprüfung ergab, daß die Erfassung von Verhaltensauffälligkeiten in dieser Form zwar ungewöhnlich ist, jedoch

nicht gegen die Vorschriften des Schulgesetzes verstößt, da es ausdrücklich die Erhebung und **Verarbeitung von Verhaltensdaten erlaubt**.

Allerdings ist die Schule unserer Empfehlung gefolgt, die Unterlagen nur bis zum Ende des Schuljahres aufzubewahren und nicht, wie zunächst beabsichtigt, bis zum Fachabitur. Wir haben die Schule außerdem aufgefordert, die Sammlung angesichts der Sensibilität der gespeicherten Daten gesondert aufzubewahren und gegen unbefugten Zugriff zu schützen.

4.9.2 Videoaufzeichnungen für Unterrichtszwecke

Im Rahmen sonderpädagogischer Kurse mit Behinderten werden durch die Staatliche Schule für Sehgeschädigte Video- und Tonaufzeichnungen von Schülerinnen und Schülern gefertigt. Dies ist nur zulässig, wenn die Betroffenen eingewilligt haben.

Die Staatliche Schule für Sehgeschädigte fertigt bei Bedarf von Teilnehmern an Trainings- und Förderkursen der Schule **Videoaufzeichnungen**, um diese nach Abschluß der jeweiligen Trainingseinheit zur Reflexion der Kursarbeit im Rahmen der pädagogischen Beratung zu verwenden. Auch im Bereich der Lehrerfortbildung und zur Information über die sonderpädagogische Arbeit der Schule werden diese Aufnahmen eingesetzt.

Der Datenschutzbeauftragte der Schule bat uns um Beratung, ob es erforderlich sei, für jeden neuen Kurs, in dem Videoaufnahmen vorgenommen werden, eine **Einverständniserklärung** durch Erziehungsberechtigte oder volljährige Betroffene einzuholen oder ob eine Einverständniserklärung für den gesamten Betreuungszeitraum, unter Umständen vom Vorschulalter bis in die Volljährigkeit hinein ausreiche.

Wir haben nach intensiven Gesprächen mit dem Datenschutzbeauftragten der Schule und der Schulleitung zu einer jeweils besonderen Einverständniserklärung geraten. Diese Empfehlung wurde mittlerweile von der Schule umgesetzt. Ferner wird von der Staatlichen Schule für Sehgeschädigte sichergestellt, daß die Videobänder in einem **gesonderten Schrank** aufbewahrt werden und die Notwendigkeit der Speicherung in regelmäßigen Abständen überprüft wird. Sind die Aufnahmen nicht mehr zur Aufgabenerfüllung erforderlich, werden sie gelöscht.

In diesem Zusammenhang wurde wiederum deutlich, daß die Bestellung eines **behördlichen Datenschutzbeauftragten** unsere Zusammenarbeit mit den öffentlichen Stellen erleichtert, da er mit seinem Wissen über die Verwaltungsabläufe in der öffentlichen Stelle Schwachpunkte im Datenschutz finden und selbst oder mit unserer Unterstützung beseitigen kann.

4.9.3 Der gestohlene PC

Zu den Datensicherungsmaßnahmen gehört es auch, zu verhindern, daß ein PC aus den Räumlichkeiten der Verwaltung entwendet wird. Lasche Datensicherungsmaßnahmen erhöhen das Risiko von PC-Diebstählen und führen zum Verlust gespeicherter Daten.

Eine Studentenvertretung unterrichtete uns darüber, daß aus dem **Verwaltungsbereich einer Hochschule** ein PC entwendet worden war, auf dessen Festplatte Namen und Anschriften von Studenten, wissenschaftlichen und nichtwissenschaftlichen Mitarbeitern sowie Professoren und Lehrern gespeichert waren. Auf unsere Nachfrage teilte uns die Hochschule mit, daß der **PC** aus der Aktenregistratur der zentralen Hochschulverwaltung **abhanden gekommen** sei, ohne daß Anhaltspunkte für eine Gewaltanwendung festgestellt werden konnten. Üblicherweise sei dieser Raum stets verschlossen. Seitens der Hochschule konnte keine Erklärung für den Verlust des PC gefunden werden.

Wir mußten deshalb davon ausgehen, daß die Hochschule **keine ausreichenden Zugangsschutzmaßnahmen** getroffen hatte. Diesen Verstoß haben wir beanstandet und zugleich der Hochschule Empfehlungen und Hinweise gegeben, wie sie zukünftig mit einfachen Sicherungsmaßnahmen die Gefahr eines PC-Diebstahls minimieren und durch Verschlüsselung der gespeicherten Informationen der Verletzung schutzwürdiger Belange vorbeugen kann. Inzwischen erarbeitet die Verwaltung der Hochschule neue Regelungen zum Datenschutz und zur Datensicherheit.

5. Datenschutz bei den Gerichten

5.1 Haftbefehle im Mülleimer

Immer wieder erweist sich bei den Behörden die Entsorgung von Altpapier als datenschutzrechtliche Schwachstelle.

Ein Bürger staunte nicht schlecht, als er bei dem Versuch, „schnell mal etwas wegzuwerfen", in der am Straßenrand stehenden **Mülltonne** mehrere Papierbögen entdeckte, die eine merkwürdige rosa Färbung besaßen, die ihm bekannt vorkam. Bei näherem Hinsehen entpuppten sie sich tatsächlich als **Haftbefehlsformulare**, in die bereits die Daten der Betroffenen eingetragen waren. Zwar hatte der Richter die Haftbefehle noch nicht gesiegelt und unterschrieben, so daß eine mißbräuchliche Verhaftung nicht möglich gewesen wäre. Zu kritisieren blieb hier jedoch, daß wieder einmal sensible Informationen über Mitbürger durch Unachtsamkeit Unbefugten zur Kenntnis gelangen konnten. Aus den Formularen war nämlich für jedermann ersichtlich, daß die Betroffenen zur Abgabe der eidesstattlichen Versicherung bei Gericht vorgeladen worden waren.

Das Besondere an dieser Panne war, daß sie **trotz organisatorischer Vorkehrungen** und Vorschriften über den Umgang mit Altpapier geschehen konnte. So existierte eine ausdrückliche Anweisung an das Reinigungspersonal, den Inhalt der Papierkörbe in den Geschäftsstellen und Arbeitszimmern nicht einfach in die Mülltonne, sondern in gesonderte Container zu entleeren, die von einer Spezialfirma entsorgt wurden. Dem Reinigungspersonal war jedoch nicht klar gewesen, daß in diese Vorsichtsmaßnahmen auch die Papierkörbe in den Sitzungssälen miteinzubeziehen waren. Auch diese Lücke im System ist nunmehr jedoch geschlossen.

5.2 Prozeßkostenhilfeanträge nicht an die Gegenseite

Der Bundesgesetzgeber hat endlich klar geregelt, was die Datenschutzbeauftragten jahrelang gefordert haben: Persönliche und insbesondere Vermögensverhältnisse dürfen dem Prozeßgegner nicht mehr ohne weiteres bekannt gemacht werden.

In der Vergangenheit (16. TB, S. 66) und auch im laufenden Berichtsjahr hatten sich immer wieder Bürger beschwert, die im Verfahren zur Gewährung einer Prozeßkostenhilfe ihre Vermögensverhältnisse offenlegen und dann mit ansehen mußten, wie diese **sensiblen Erklärungen** der **Gegenpartei zugänglich** gemacht wurden. Obwohl die Rechtsprechung schon seit längerer Zeit klargestellt hatte, daß dies nur in eingeschränktem Maße zulässig sei, fehlten bislang eindeutige gesetzliche Vorgaben.

Diesem Zustand hat der Gesetzgeber durch eine Änderung der Zivilprozeßordnung nunmehr ein Ende bereitet. Im Prozeßkostenhilfeänderungsgesetz ist eindeutig geregelt, daß sowohl die Erklärung zur Erlangung einer Prozeßkostenhilfe als auch die dazu eingereichten Belege dem Gegner **nur mit Zustimmung** der betreffenden Partei zugänglich gemacht werden dürfen. Diese Änderung der Zivilprozeßordnung ist am 1. Januar 1995 in Kraft getreten.

6. Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung

6.1 Datenschutzverordnung in Kraft getreten – Schleswig-Holstein setzt Maßstäbe

In der neuen Datenschutzverordnung werden erstmals „Grundsätze ordnungsgemäßer Datenverarbeitung" formuliert. Für die Praktiker enthält sie konkrete Handlungsanweisungen.

Wir hatten bei der Landesregierung mehrfach die Fertigstellung der nach dem LDSG zu erlassenden Rechtsverordnung

angemahnt (vgl. 15. TB, S. 91; 16. TB, S. 71). Zur Erinnerung: Der Gesetzgeber hat im Oktober 1991 in § 7 Abs. 4 LDSG bestimmt, daß die Landesregierung „durch Verordnung die Einzelheiten einer ordnungsgemäßen automatisierten Datenverarbeitung durch öffentliche Stellen" zu regeln hat. Dabei sollte sie „insbesondere die im LDSG genannten Datensicherheitsmaßnahmen nach dem Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen fortschreiben und Anforderungen an Verfahren sowie die Dokumentation und deren Aufbewahrungsfristen" festlegen.

Das Ergebnis dieses Auftrages ist nunmehr mit der „Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (**Datenschutzverordnung** – DSVO –)" vom 12.09.1994 (GVOBl Schl.-H. S. 473) vorgelegt worden. Obwohl nicht alle Regelungsvorschläge, die wir der Landesregierung unterbreitet hatten, berücksichtigt worden sind, haben wir dieser Verordnung unsere Zustimmung nicht versagt. Wir haben uns dabei auch von der Überlegung leiten lassen, daß es sich bislang um ein Unikat handelt. **Schleswig-Holstein** hat insoweit bundesweit eine anerkennenswerte **Vorreiterrolle** übernommen und „verordnungsgeberisches" Neuland betreten.

Das der Datenschutzverordnung zugrundeliegende **Konzept** läßt sich wie folgt charakterisieren:

- **Einheitliche Regelungen für alle Behörden**

  Die Verordnung ist gleichermaßen verbindlich für Landes- und Kommunalbehörden wie auch für alle sonstigen öffentlichen Stellen, soweit sie der Landesaufsicht unterliegen, da sie an den Geltungsbereich des LDSG anknüpft. Dies führt zu einer Vereinheitlichung der (bisher in Form von divergierenden Verwaltungsanweisungen) bestehenden Regelungen zur Ordnungsmäßigkeit der Datenverarbeitung.

- **Schaffung von „Grundsätzen ordnungsgemäßer Datenverarbeitung" in Form von Mindestanforderungen**

  Durch die Verordnung werden Mindestanforderungen an die Gestaltung und Durchführung automatisierter Verwaltungsabläufe definiert, deren Unterschreiten grundsätzlich nicht akzeptabel ist, weil damit in der Regel neben Sicherheits- auch Rechtsprobleme verbunden wären (z.B. Gefahr unzulässiger Datenerhebungen bzw. Datenübermittlungen).

- **Orientierung an dem Standard, der bei „professionellen" Datenverarbeitern bereits jetzt erreicht ist**

  Es werden den Behörden keine Auflagen gemacht, die nicht bereits von vielen datenverarbeitenden Stellen erfüllt wurden, bevor die Verordnung in Kraft getreten ist.

- **Stärkung der Position der Sicherheitsverantwortlichen gegenüber den „Geldgebern"**

  Der durch die Verordnung vorgegebene Mindeststandard setzt den immer wieder festzustellenden Versuchen Grenzen, bei anstehenden IT-Investitionen die Gewichte zu Lasten der Datensicherheit und Revisionsfähigkeit der Datenverarbeitung in Richtung der Maxime „lieber billigere und dafür mehr IT-Arbeitsplätze" zu verschieben.

- **Trennung zwischen den Verantwortungsbereichen der IT-Stellen und den Verfahrensbenutzern**

  Die Entwicklung und Administration von automatisierten Verfahren wird als eine Dienstleistung angesehen, die gegenüber den Benutzern (Fachabteilungen) erbracht wird und die unabhängig ist von den eigentlichen Verwaltungsverfahren (z.B. Erlaß eines Verwaltungsaktes). Obligatorisch ist daher eine zumindest logische – in der Regel auch eine organisatorische – Abgrenzung der jeweiligen Verantwortungsbereiche zueinander.

- **Verzicht auf Formvorschriften, statt dessen Definition von Zielvorgaben**

  Der Vielgestaltigkeit der Aufgabenstellungen und der Verwaltungsabläufe in Behörden wird dadurch Rechnung getragen, daß keine bestimmten Darstellungsformen (z.B. für die Dokumentation oder Sicherheitskonzepte) vorgeschrieben werden. Die Regelungen orientieren sich am Ergebnis und fordern ansonsten „nur" die Nachvollziehbarkeit durch sachkundige Dritte.

Als wesentliche Regelungsinhalte sind zu nennen:

- **Definition des Begriffs „ordnungsgemäß"**

  Die Behörden können nur dann für sich in Anspruch nehmen, personenbezogene Daten in einem automatisierten Verfahren ordnungsgemäß zu verarbeiten, wenn

  - die Datenverarbeitung in Übereinstimmung mit dem geltenden Recht erfolgt,
  - ein Sicherheitskonzept vorliegt,
  - die Programme und Verfahren dokumentiert sind,
  - ein Test durchgeführt wurde und
  - eine Freigabe erteilt worden ist.

- **Definition der Begriffe „Programm" und „Verfahren"**

  Um das Sprachbabylon auf diesem Gebiet zu beenden, wird festgelegt, daß als Programme alle Arbeitsanweisungen

(Software) an informationstechnische Geräte (Hardware) anzusehen sind. Die Funktionsweise, die Herkunft, die Programmiersprache spielen also keine Rolle. Es kommt nur auf die Tatsache an, daß die Anweisungen Einfluß auf das Ergebnis der maschinellen Verarbeitung haben können. „Automatisierte Verfahren" sind nicht nur die Summe mehrerer Programme, sondern die gesamten Arbeitsabläufe mit Hilfe automatisierter Datenverarbeitung. Sie umfassen also Hardware, Software und Orgware.

– **Pflicht zur Erstellung einer nachvollziehbaren Dokumentation**

Die Verordnung legt fest, daß die Dokumentation eines automatisierten Verfahrens mindestens eine Beschreibung

- der jeweiligen Aufgaben,
- des Verfahrensablaufs einschließlich der Darstellung der eingesetzten Programme und
- des Programm- und Verfahrenstests

enthalten muß. Diese Dokumentation ist nach jeder Änderung von Programmen oder Verfahrensabläufen fortzuschreiben. Sie muß so gestaltet sein, daß sie für sachkundige, nicht am automatisierten Verfahren beteiligte Personen nachvollziehbar ist.

– **Festlegung der Aufbewahrungsvorschriften für die Dokumentation**

Es werden drei Fallgruppen unterschieden:

- Verfahren, bei denen die Ergebnisse der maschinellen Verarbeitung vollständig in Papierform vorliegen: Die Unterlagen sind mindestens solange aufzubewahren, wie mit den betreffenden Programmen auf die Daten zugegriffen werden kann.
- Verfahren, die Datenbestände erzeugen, die ausschließlich in automatisierten Dateien abgelegt werden: Die Aufbewahrungspflicht für die Dokumentation besteht bis zum Zeitpunkt der Löschung (oder des Ausdrucks) der Daten.
- Verfahren, mit denen Daten an andere Stellen übermittelt werden: Die Mindestaufbewahrungsdauer ist auf sechs Jahre festgelegt. Das gilt nicht, wenn die übermittelten Daten (beim Absender) „in lesbarer Form vorhanden sind".

– **Sonderregelung für die Dokumentation von Fremdsoftware**

Die Dokumentationspflicht bezieht sich nicht auf Software, die die datenverarbeitende Stelle nicht selbst entwickelt, sondern an der sie nur Nutzungsrechte erworben hat. In der

entsprechenden Regelung der Verordnung kommt der Grundsatz zum Tragen, daß die datenverarbeitenden Stellen nur diejenigen Elemente eines automatisierten Verfahrens zu dokumentieren haben, die sie selbst ändern können.

– **Sicherheitskonzepte**

Alle technischen und organisatorischen Sicherheitsmaßnahmen sind in Sicherheitskonzepten festzulegen. In ihnen sind die tatsächlichen örtlichen und personellen Gegebenheiten zu berücksichtigen. Außerdem ist festzulegen, in welchem Umfang Protokollierungen über die Nutzung der Verfahren (Übermittlungs-, Zugriffs-, Eingabekontrollen) vorzunehmen sind. Die Unterlagen enthalten somit die Sicherheitsvorgaben, deren Berücksichtigung bzw. Einhaltung im Rahmen der Freigaben und des praktischen Einsatzes der Verfahren zu überprüfen ist.

– **Risikoanalysen**

Werden personenbezogene Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen oder die sonst als besonders schutzwürdig gelten, automatisiert verarbeitet, ist neben der Darstellung der Sicherheitsmaßnahmen in einer Risikoanalyse zu beschreiben, welche Risiken aus welchen Gründen nicht oder nur zum Teil durch getroffene Schutzmaßnahmen ausgeschlossen werden können. Damit sind Sicherheitslücken nicht mehr nur Sache der Techniker. Die Verantwortung für die Risiken liegt bei der Leitung der datenverarbeitenden Stelle. Sie kann sich nicht auf Unwissenheit berufen, da die Risikoanalysen Teil der freigegebenen Verfahrensbeschreibung sind.

– **Trennung zwischen der Administration und der Benutzung automatisierter Verfahren, Pflicht zur Kontrolle der Systembetreuer**

Durch technische und organisatorische Maßnahmen ist sicherzustellen, daß verändernde Zugriffe auf Programme zur Systemsteuerung und auf freigegebene Anwendungsprogramme und Verfahren nur durch dazu ausdrücklich befugte Personen erfolgen können. Diese Systembetreuer sind durch weisungsbefugte Mitarbeiter oder deren Beauftragte zu kontrollieren. Diese Trennungs- und Überwachungspflicht gilt nicht für „persönliche", gleichwohl dienstliche IT-Geräte (z.B. PC eines Richters).

– **Pflicht zur Dateiverschlüsselung**

Dateien auf Datenträgern mobiler Geräte (Laptops, Notebooks und dergleichen), die von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten eingesetzt werden,

sind zu verschlüsseln. Damit soll dem erhöhten Risiko einer unbefugten Kenntnisnahme von Daten nach einem Verlust der Geräte (z.B. durch Diebstahl) entgegengewirkt werden (vgl. 16. TB, S. 73).

– **Pflicht zum Test und zur Freigabe**

Die in einem automatisierten Verfahren eingesetzten Programme (soweit es sich nicht um Fremdsoftware handelt) sowie das gesamte Verfahren sind vor Aufnahme der Verarbeitung personenbezogener Daten daraufhin zu testen, ob die in den Vorgaben festgelegten Ergebnisse erzielt werden. Mit der anschließenden Freigabe übernimmt die datenverarbeitende Stelle die Verantwortung für die Ordnungsmäßigkeit des Verfahrens.

– **Übergangsregelungen**

Die Verordnung ist am 13.09.1994 in Kraft getreten. Bereits eingesetzte Verfahren müssen die in ihr festgelegten Anforderungen jedoch erst spätestens fünf Jahre nach dem Inkrafttreten erfüllen. Die Dokumentations-, Test- und Freigabepflichten gelten für Programm- und Verfahrensänderungen allerdings davon abweichend bereits ab April 1995.

Unsere Prüfungs- und Beratungsaktivitäten in den Bereichen „Datensicherheit" und „Ordnungsmäßigkeit der Datenverarbeitung" werden durch diese Verordnung auf eine neue Grundlage gestellt. Zwar enthält sie keine Regelungen, die nicht unseren bereits in der Vergangenheit erhobenen Forderungen entsprechen. Der in der öffentlichen Verwaltung für erforderlich und angemessen gehaltene Sicherheits- und Revisionsstandard ist jedoch nunmehr rechtsverbindlich festgeschrieben worden. Es muß von den datenverarbeitenden Stellen erwartet werden, daß sie in Zukunft weniger um einzelne Maßnahmen feilschen, sondern statt dessen handeln (vgl. hierzu z.B. Tz. 6.4.1).

Über die Erfahrungen mit dieser neuen Rechtsmaterie wird in den nächsten Jahren zu berichten sein.

6.2 Ergebnisse von Prüfungsmaßnahmen im Bereich der automatisierten Datenverarbeitung

6.2.1 Beanstandungen akzeptiert – Abhilfe auf die lange Bank geschoben (2. Aufl.)

Nach Kontrollen bei der Stadt Kiel und bei der Stadt Flensburg wurden Mängel eingeräumt und Abhilfe versprochen. Geschehen ist aber bis heute nicht allzuviel.

Erstmals in der nunmehr 17jährigen Praxis des Landesbeauftragten ist ein Sachverhalt im Tätigkeitsbericht genauso überschrieben wie im Jahr zuvor. **„Beanstandungen akzeptiert – Abhilfe auf die lange Bank geschoben"** hieß es bereits auf S. 77 des 16. Tätigkeitsberichtes. Die Wiederholung ist angezeigt, weil sich im Laufe des letzten Jahres an dem dargestellten Problem nichts geändert hat.

Im Jahr 1992 haben wir bei der **Landeshauptstadt Kiel** eine datenschutzrechtliche Prüfung durchgeführt (vgl. 15. TB, S. 89). In einer Stellungnahme vom Mai 1993 wurden die **Beanstandungen** und **Vorschläge** zur Behebung der Mängel und zur Verbesserung des Datenschutzes von der Stadt **weitgehend akzeptiert**. Über die Zeitpunkte der Realisierung wurden jedoch keine konkreten Angaben gemacht. Das war nicht verwunderlich, denn es lagen noch nicht einmal die Äußerungen aller Fachämter vor. Eine weitere Stellungnahme vom Oktober 1993 wiederholte faktisch die Aussagen, die 5 Monate früher auch schon getroffen worden waren. Selbst persönliche Kontakte des Landesbeauftragten mit dem Oberbürgermeister hatten keinen Einfluß auf die offensichtliche **Verzögerungstaktik** einiger Fachämter wie Zitate aus einem Schreiben des Oberbürgermeisters vom September 1994 belegen:

- „Die Beantwortung bzw. Umsetzung ... verzögert sich durch einen Brandanschlag ...".
- „Die Beantwortung ... verzögert sich aus personellen Gründen".
- „Die Stellungnahmen ... werden im Oktober erwartet." (Anm.: Sie sind offensichtlich bisher nicht beim Oberbürgermeister eingegangen, jedenfalls sind wir noch nicht unterrichtet worden).
- „Es werden ... Dienstanweisungen erstellt.".
- „Die Raumsituation konnte bisher nicht grundlegend verbessert werden."
- „Als zentrales Problem steht ferner noch ... aus."

Was uns mit Sorge erfüllt, ist die Tatsache, daß sich die Abarbeitung unserer Beanstandungen aufgrund einer datenschutzrechtlichen Überprüfung im September 1993 bei der **Stadt Flensburg** (vgl. 16. TB, S. 79) möglicherweise ähnlich entwickelt.

In ihrer Stellungnahme vom April 1994 hat auch die Stadt Flensburg die festgestellten datenschutzrechtlichen Mängel und den sich daraus ergebenden Handlungsbedarf bestätigt. Weiterhin wurde eine **Vielzahl von Absichtserklärungen** abgegeben. Die Formulierungen gleichen denen der Stadt Kiel teilweise aufs Wort:

- „Wir werden die erforderlichen Anweisungen und Regelungen jetzt neu festlegen."
- „Wir werden jetzt damit beginnen ... ."

- „Zu datenschutzrechtlichen Maßnahmen in den Fachämtern werden wir gesondert Stellung nehmen."
- „Wir werden ... die sich daraus ergebenden Maßnahmen umsetzen."
- „Wir bemühen uns, ..."
- „Wir stimmen mit Ihnen überein, daß der Zeitpunkt erreicht ist, formelle Grundlagen für eine Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen zu schaffen ... . Wir werden ein Konzept entwickeln ... ."
- „Über die Umsetzung der aufgezeigten Maßnahmen werden wir Ihnen berichten."

Allerdings ist auch in diesem Fall bis zum Ende des Berichtszeitraums noch nichts Konkretes geschehen. Jedenfalls hat man uns nicht entsprechend unterrichtet.

Zwei **Schlußfolgerungen** gilt es aus diesen Gegebenheiten zu ziehen:

- Unsere Prüfungsmaßnahmen sind, wie man so schön sagt, „für die Katz", wenn die geprüften Stellen uns in bezug auf die festgestellten Mängel Recht geben, es aber damit bewenden lassen.
- Die betreffenden Behörden verarbeiten personenbezogene Daten in Kenntnis der Mißachtung bindender gesetzlicher Vorschriften und tun über einen längeren Zeitraum nichts, um diesen Zustand zu ändern.

Beides ist nicht hinnehmbar. Der Gesetzgeber wird sich fragen müssen, ob in dem Landesdatenschutzgesetz für derartige Fälle nicht doch Sanktionen hätten vorgesehen werden müssen. Besonders bemerkenswert ist die zögerliche Haltung der **Stadt Kiel** aus zwei Gründen. Die Stadt hat die Absicht umfangreicher weiterer Automatisierungsvorhaben bekundet. Da sollte man erwarten können, daß zuvor die Verfahrensregeln in dem erforderlichen Maße geschaffen oder überarbeitet werden. Zum anderen möchte die Stadt ihre Verwaltung modernisieren, d.h. leistungsstärker und effizienter gestalten. Die bislang gezeigte Reaktion auf unsere Beanstandungen entspricht diesem Ideal noch in keiner Weise.

6.2.2 Kontrolle der Medizinischen Universität zu Lübeck abgeschlossen

Die Kontrolle der Datenverarbeitung im Klinikum der Medizinischen Universität zu Lübeck ergab Sicherheitsmängel und schwerwiegende Rechtsprobleme bei der Forschung mit Patientendaten.

Im 16. Tätigkeitsbericht (S. 83) ist darüber berichtet worden, daß im Herbst 1993 eine Prüfungsmaßnahme im Klinikum der Medizinischen Universität zu Lübeck (MUL) abgebrochen

werden mußte, weil keine ausreichend prüffähigen Unterlagen über die installierten Datenverarbeitungsgeräte und die benutzte Software vorgelegt werden konnten. Deshalb wurden der MUL zunächst nur die Teilergebnisse der Prüfung mitgeteilt und sie zur Stellungnahme und Behebung der Mängel aufgefordert. Der überwiegende Teil der **Beanstandungen** und der **Verbesserungsvorschläge** wurde seitens der MUL akzeptiert und umfangreiche **Absichtserklärungen** abgegeben.

Der zweite Teil der Prüfung bezog sich auf die konkreten Datenverarbeitungsabläufe in sechs **ausgewählten Kliniken** und **Instituten** (von insgesamt über 40).

Dabei zeigte sich, daß die Ergebnisse der ersten Teilprüfung auch sechs Monate später noch keine wesentlichen Auswirkungen auf die Organisation, Absicherung und Überwachung der automatisierten Verarbeitung der Patientendaten gehabt haben. Positive Ansätze waren lediglich in zwei der überprüften Organisationseinheiten festzustellen.

Die einzelnen **Beanstandungen** lassen sich zu folgenden Schwerpunkten zusammenfassen:

- Es stellt die MUL vor offenbar kaum zu lösende organisatorische Probleme, den tatsächlichen Einsatz der ca. 600 vernetzten und unvernetzten PC im Klinikum zu erfassen und zu ermitteln, auf welchen Geräten welche personenbezogenen Daten zu welchen Zwecken mit welchen Programmen verarbeitet werden. Ein dem Prüfer als authentisch übergebenes **Geräteverzeichnis** erwies sich als **unvollständig** und bereits während der Prüfung als **überholt** (6 Wochen nach der Erstellung des Verzeichnisses).
- Die vorgelegten **Dateibeschreibungen** waren nach wie vor überwiegend falsch, unvollständig oder für Dritte inhaltlich nicht nachvollziehbar.
- Die tatsächlich realisierten **Datensicherungsmaßnahmen** konnten insgesamt **nicht** als **angemessen** angesehen werden.
  - Es bestehen weder allgemeine noch (mit einer Ausnahme) klinikspezifische Sicherheitskonzepte.
  - Die Übernahme und weitere Nutzung von Daten aus Patientenakten in „Sekundärdatenbestände" (Dateien in PC) wird teilweise nicht wirksam überwacht.
  - PC und Datenträger sind in vielen Fällen unzureichend gegen eine unbefugte Entfernung aus dem Bereich des Klinikums gesichert.
  - Als unzulänglich ist auch die Sicherung der PC gegen unbefugte Nutzungen anzusehen.
  - Auf eine „Sicherung durch Anonymisierung" wurde vielfach verzichtet, obwohl dies ohne Einschränkung der Qualität der medizinischen Versorgung möglich wäre.
- Im Zusammenhang mit der **Überwachung** der **ordnungsgemäßen Anwendung** der **Datenverarbeitungsprogramme** ist noch immer nicht geklärt, wer im Innenverhältnis für

die Überwachung der Einhaltung der gesetzlichen Vorgaben verantwortlich ist bzw. auf wen diese Überwachungsfunktionen delegiert sind.

- Die Kontrollaufgaben der **klinikinternen Datenschutzbeauftragten** sind überwiegend gar nicht oder nur unvollständig definiert.
- Für das Installieren von Computern und das Anlegen von Datenbeständen besteht in der Regel **keine Genehmigungspflicht**.
- Die **Nutzung von Patientenakten** zum Aufbau von automatisierten Datenbeständen, die nicht unmittelbar der medizinischen Versorgung dienen, wird im allgemeinen **nicht überwacht**.
- Viele Datenbestände unterliegen **keiner effektiven Nutzungskontrolle**. Das gilt in vielen Fällen auch für Patientenakten.

Die Zielrichtung der Prüfungsmaßnahme war ausgerichtet auf die **Sicherheitsaspekte** im Zusammenhang mit der personenbezogenen Datenverarbeitung. Bei den Erhebungen zur Sicherung von Datenbeständen, die im Rahmen der medizinischen Versorgung der Patienten angelegt worden sind, waren jedoch **grundsätzliche rechtliche Problemstellungen** bezüglich der Nutzung dieser Datenbestände zum Zwecke der Forschung und Lehre unübersehbar.

- In einem signifikanten Umfang werden personenbezogene Daten, die im Rahmen der medizinischen Versorgung von Patienten erhoben worden sind, von Personen, die nicht an der Behandlung als Konsiliarärzte oder ärztliches Hilfspersonal beteiligt gewesen sind, später zu **Forschungszwecken** genutzt bzw. gelangen diesen Personen zur Kenntnis.
- Nur in wenigen Fällen (gemessen an der Gesamtzahl) haben die Patienten hierzu ihre **Einwilligung** gegeben.
- Auch wenn keine Einwilligungen erteilt worden sind, werden die Daten im weiteren Verlauf der Forschungsarbeiten gar **nicht** oder nur **unzureichend anonymisiert**.
- Die Verfahrensweisen sind „gängig" und der **Leitung** des Klinikums und dem Rektorat der MUL offenbar **bekannt**.
- Es werden zwar zwingende Notwendigkeiten für diese Verfahrensweisen geltend gemacht, **Alternativen** wurden jedoch offenbar **nicht** von allen Beteiligten **eingehend untersucht** und realisiert.

Die Rechtslage stellt sich wie folgt dar:

- § 4 der **Berufsordnung der Ärztekammer** Schleswig-Holstein legt als vorrangiges bereichsspezifisches Recht zur Schweigepflicht der Ärzte u.a. fest: „Zum Zwecke der wissenschaftlichen Forschung und Lehre dürfen die der Schweigepflicht unterliegenden Tatsachen und Befunde nur

soweit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt".

- Das Landesdatenschutzgesetz läßt eine **zweckändernde Nutzung** von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ohne Einwilligung Betroffener nur zu, wenn eine Rechtsvorschrift dies erlaubt oder im Einzelfall zwingend voraussetzt.
- **§ 203 Strafgesetzbuch** stellt denjenigen unter Strafe, der als Arzt ... unbefugt ein fremdes Geheimnis ... offenbart.

Ohne näher auf die strafrechtlichen Aspekte einzugehen, haben wir die Verfahrensweise aus datenschutzrechtlichen Gründen **beanstandet**. Im Hinblick darauf, daß nach Aussage der befragten Ärzte der MUL in vergleichbaren Universitätskliniken gleich oder zumindest ähnlich verfahren wird, liegt hier offenbar ein **Grundsatzproblem** vor, zu dessen Lösung die Ministerin für Wissenschaft, Forschung und Kultur um ein Votum gebeten wurde.

In ihrer Stellungnahme hat die MUL die **Beanstandungen akzeptiert**. Zur Lösung der Probleme hat sie einen **„externen"** behördlichen **Datenschutzbeauftragten bestellt**. Man erhofft sich offenbar von diesem neutralen Fachmann die Durchschlagskraft, die erforderlich ist, um die widerstreitenden Interessen innerhalb des Klinikums unter einen datenschutzrechtlichen Hut zu bringen. Uns ist ein **Aktivitäten-** und **Maßnahmenkatalog** für 1995 vorgelegt worden. Er umfaßt 46 Positionen. Werden sie alle termingerecht umgesetzt, wird man dem vom Gesetzgeber geforderten Sicherheitsniveau ein gutes Stück näher gekommen sein. Wir werden den Fortgang dieser Arbeiten konstruktiv-kritisch begleiten.

6.2.3 Ein etwas anderes Prüfungsergebnis

Eine Kontrolle bei der Stadt Norderstedt hat ergeben, daß dort in weiten Bereichen vorbildliche Regelungen zum IT-Einsatz bestehen. An der konsequenten Umsetzung mangelte es in Teilbereichen.

Es kommt nicht eben häufig vor, daß von einer datenverarbeitenden Stelle zu Beginn einer Datenschutzkontrolle ganz selbstverständlich ein aktuelles EDV-Konzept, eine allgemeine Dienstanweisung für die elektronische Datenverarbeitung, eine spezielle Dienstanweisung über den Einsatz und die Nutzung von PC und eine vollständige Dokumentation über die Benutzer im PC-Netz und ihre Befugnisse präsentiert werden. Auch inhaltlich konnten die unserem Prüfer von der **Stadt Norderstedt** vorgelegten Unterlagen den **datenschutzrechtlichen Anforderungen weitgehend genügen**. Hierzu einige Beispiele:

- Die Stadt geht richtigerweise davon aus, daß die Unterstützung der Verwaltungsarbeit durch Datenverarbeitungsver-

fahren „einen langen und schrittweisen Änderungsprozeß erfordert, der nicht nur geräte-, verkabelungs- und programmtechnisch vollzogen werden muß, sondern auch mit Änderungen im Aufbau und im Ablauf der Verwaltung verbunden ist".

- Sie will den Weg zur technikunterstützten Informationsverarbeitung sowohl auf der Ebene der Endgeräte als auch auf der Ebene der Anwendungen und der Ebene der Vernetzung vollziehen.
- Vor der Einführung und Änderung von EDV-Verfahren in einem Fachamt wird unter Beteiligung einer Arbeitsgruppe „Automation" durch die Organisationsabteilung die Zweckmäßigkeit des EDV-Einsatzes geprüft.
- Neue EDV-Verfahren sind vom jeweiligen Fachamt zu prüfen und freizugeben. Die Form der Überprüfung und das Ergebnis sind schriftlich festzuhalten und dem Hauptamt und dem Rechnungsprüfungsamt mitzuteilen.
- Die „Einrichtung" von Benutzern und die Festlegung ihrer Rechte erfolgt zwar durch die EDV-Abteilung. Die Personen und ihre Befugnisse werden aber durch die jeweiligen Fachämter bestimmt.
- Die Mitarbeiter, die EDV-Anlagen und EDV-Verfahren nutzen dürfen, erhalten zu Beginn ihrer Tätigkeit ein persönliches Kennwort.
- Es dürfen nur solche Daten erfaßt werden, die in der entsprechenden Dateibeschreibung genannt sind. Nach dem Anlegen neuer Dateien ist das Rechnungsprüfungsamt zwecks Meldung der Datei an den Landesdatenschutzbeauftragten zu informieren.
- Die Bedienung der zentralen EDV-Anlage erfolgt ausschließlich durch die Systemkoordinatoren. Die Bedienungsvorgänge sind zu protokollieren. Der Zutritt zum EDV-Raum ist nur befugten Mitarbeitern gestattet.
- Die Zuständigkeit zwischen der EDV-Abteilung im Hauptamt und den Fachämtern bezüglich der Datensicherung ist durch eine abschließende Aufzählung eindeutig abgegrenzt.
- Die Beschaffung von EDV-Programmen für PC darf nicht ohne Beteiligung der Arbeitsgruppe „Automation" erfolgen. Die Erstellung eigener Software für PC durch Mitarbeiter der Stadt ist grundsätzlich untersagt.
- PC sind nach Möglichkeit in ein Netzwerk einzubinden, um die Zugriffsmöglichkeiten auf Datenbestände zu beschränken und Datensicherung besser zu gewährleisten.

Diese Vorgaben entsprechen also im wesentlichen den Regelungen in der neuen Datenschutzverordnung (vgl. Tz. 6.1 dieses Berichtes). Trotzdem mußten auch gegenüber dieser geprüften Stelle **Beanstandungen** ausgesprochen werden. Es mangelte nämlich in einigen Bereichen an der konsequenten Umsetzung der Erkenntnisse und Absichten, die man selbst „für gut und richtig" hält, in die Praxis.

Die Ursachen lagen offensichtlich nicht in Unkenntnis, Fahrlässigkeit oder mangelndem Engagement der Mitarbeiter, sondern in **„Kapazitätsgrenzen"**. Das machen folgende Zahlen deutlich. Es wurden von der Stadt zum Zeitpunkt der Prüfung

- 8 Rechnersysteme mit über
- 180 Endgeräten unter der Steuerung von
- 4 verschiedenen Betriebssystemen zur Abwicklung von
- 23 automatisierten Verfahren in
- 29 (von insgesamt 34) Ämtern bzw. Abteilungen

eingesetzt.

Das Management für diese nicht gerade kleine „IT-Welt" sollte von nur einem Abteilungsleiter und zwei Sachbearbeitern bewältigt werden. Die Folge war, daß man wegen der **„kurzen Personaldecke"** notgedrungen nach der Devise arbeitete, „erst einmal den Betrieb aufrechterhalten und ausbauen – alles andere ist zweitrangig". So blieben Mängel in der Dokumentation, der Datensicherheit und hinsichtlich der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme nicht aus.

Unsere **Vorschläge** zur Behebung der Mängel und zur Verbesserung des Datenschutzes wurden von der Stadt überwiegend **akzeptiert**. Bezüglich der Angemessenheit von konkreten Datensicherheitsmaßnahmen und der Wirksamkeit von Überwachungsfunktionen hat sie unserer Auffassung in einer ersten Stellungnahme widersprochen. Insoweit besteht also noch Erörterungsbedarf.

Ungeachtet dieser in Teilbereichen durchaus unterschiedlichen Beurteilung der festgestellten Sachverhalte und Kritikpunkte kann man der Stadt Norderstedt nur empfehlen, auf dem **eingeschlagenen Weg weiterzumachen**. Wenn es möglich ist, Hard- und Softwareinvestitionen in Größenordnungen von mehreren hunderttausend Mark zu tätigen, müßte es auch möglich sein, so viel Geld in die „Brainware" (sprich: in Personal) zu investieren, daß die richtigen Vorsätze auch in die Tat umgesetzt werden können. Ein gut ausgebildeter und motivierter IT-Mitarbeiter bringt sicher eine höhere Produktivitätssteigerung als zehn zwar funktionierende, aber schlecht organisierte (gesicherte) Bildschirmarbeitsplätze (wegen der ähnlichen Problemstellung vgl. auch Tz. 6.2.4 dieses Berichtes).

6.2.4 Technische und organisatorische Anforderungen an ein „Ministeriumsrechenzentrum"

Die Automatisierung der Datenverarbeitung in der Verwaltung bedarf gründlicher konzeptioneller, sicherheitstechnischer und organisatorischer Vorarbeiten. In der Praxis müssen die Regelungen auch tatsächlich eingehalten werden.

Anders als im kommunalen Bereich und für die sonstigen öffentlichen Stellen bestehen seit einigen Jahren für den Landesbereich recht **detaillierte Verfahrensvorschriften** für den Einsatz informationstechnischer Systeme (IT-Systeme). Es sind dies im wesentlichen

- die IT-Richtlinien,
- die IT-Planungsgrundsätze,
- die IT-Verfahrensregelung und
- das IT-Leitstellenkonzept.

Nach dem IT-Leitstellenkonzept, das auf einem Beschluß der Staatssekretärskonferenz vom Juni 1987 beruht, haben die Ministerien ihre automatisierte Datenverarbeitung mittels sogenannter **IT-Leitstellen** zu organisieren. Die Aufgaben dieser neuen Organisationseinheiten sind:

- Beratung der Benutzer von IT-Systemen,
- Planung von IT-Anwendungen,
- Programmentwicklung für dezentrale Fachanwendungen sowie Büroautomations- und Kommunikationslösungen auf Abteilungsrechnern und Arbeitsplatzendgeräten,
- Beschaffung von Hard- und Software,
- Betrieb der örtlichen IT-Systeme.

Dieses Aufgabenspektrum umfaßt prinzipiell die gleichen Geschäftsfelder, die auch die „große" Datenzentrale abdeckt. So lag es nahe, nach Abschluß der Prüfung bei der Datenzentrale (vgl. 16. TB, S. 76) durch eine Nachschau vor Ort festzustellen, wie in IT-Leitstellen die datenschutzrechtlichen Problemstellungen in bezug auf die Datensicherheit und die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme gelöst worden sind. Kurz gesagt: Wie sind die neuen Dienstleistungseinheiten **"Ministeriumsrechenzentrum"** aufbau- und ablauforganisatorisch mit den auftraggebenden Fachabteilungen verknüpft worden. Hierfür ausgewählt wurde die IT-Leitstelle der **Ministerin für Natur und Umwelt**. Es ergaben sich folgende Erkenntnisse:

- Von einem Referenten und zwei Sachbearbeitern werden fünf Rechnersysteme und ca. 70 Arbeitsplatzendgeräte unter der Steuerung von drei Betriebssystemen und ca. 20 Softwarepaketen bzw. automatisierten Verfahren betreut.
- Aus nicht nachvollziehbaren Gründen ist ein Teilbereich der Datenverarbeitung im Ministerium für Natur und Umwelt mit 8 Terminals und 48 „Anwendungen" der Zuständigkeit der IT-Leitstelle entzogen.
- Neben der Beachtung der vorgenannten allgemeinen Regelungen obliegt es der IT-Leitstelle, auch das spezielle IT-Konzept des Ministeriums für Natur und Umwelt aus dem Jahre 1991 umzusetzen.
- Dieses Konzept enthält relativ konkrete grundsätzliche Anweisungen zu den Problembereichen: IT-Beauftragte in den

Fachabteilungen, automatisierte Textbearbeitung, Schulung und Datenschutz.

- Zum Thema Datenschutz ist darin z.B. folgendes ausgeführt: „Mit dem Ausbau des DV-Systems im Ministerium muß die Entwicklung eines Datenschutzkonzeptes verbunden sein. Hierzu ist es erforderlich, sukzessive für die Datenverarbeitung auf den Abteilungsrechnern und an den jeweiligen Arbeitsplätzen eine **Risikoanalyse** zu erstellen und darauf aufbauend ein **angepaßtes Schutzkonzept** zu entwickeln. Schwerpunktmäßig müssen noch in diesem Jahr (1991) die Arbeiten für ein Schutzkonzept für die Bereiche Texterstellung und -speicherung, Systemadministration Abteilungsrechner, Datenhaltung auf Abteilungsrechner (Datenbank) und PC im Netz begonnen werden."

Bezüglich der **Umsetzung** dieser Vorgaben in die Praxis waren **Defizite** jedoch nicht zu übersehen. Zum Zeitpunkt der Prüfung waren z.B. folgende Mängel festzustellen:

- Nicht alle eingesetzten Verfahren waren dokumentiert.
- Nicht in allen Fällen waren die Tests und die Freigabe durch die Fachabteilung erfolgt.
- Ein Datenschutzkonzept lag noch nicht vor.
- Das gleiche gilt für das Schulungskonzept.
- Auch verfahrensspezifische Risikoanalysen und Schutzkonzepte sind nicht erstellt worden.
- Mehrere, auch von der geprüften Stelle für erforderlich gehaltene ablauforganisatorische Regelungen waren noch nicht fertiggestellt.
- Einerseits hat die IT-Leitstelle einen unbeschränkten und unkontrollierbaren Zugriff auf alle Datenbestände, andererseits hat sie keinen Einfluß auf die Datensicherungsmaßnahmen in den Fachabteilungen.
- Aufträge der Fachabteilungen an die Leitstelle waren nicht immer schriftlich fixiert.
- Die Leitstelle sah sich selbst personell nicht in der Lage, alle ihr auferlegten Weisungen und Vorgaben zu erfüllen.

Dieser Umstand hatte eine Reihe **datenschutzrechtlicher Beanstandungen** zur Folge. Die Ministerin für Natur und Umwelt hat in einer ersten Stellungnahme die von uns gegebenen Empfehlungen begrüßt. Sie würden „sowohl der Abklärung der genauen praktischen Ausgestaltung von Datenschutzmaßnahmen als auch der Klärung von Verantwortlichkeiten, damit auch dem Schutz der in der IT-Leitstelle tätigen Personen" dienen. Im Laufe des Jahres 1994 seien bereits **Maßnahmen zur Verbesserung** der Situation **ergriffen** worden:

- Die Datenzentrale werde künftig Systemaufgaben unterstützen.
- Durch Umsetzung sei die Systemunterstützung personell verstärkt worden.

- Im Vorgriff auf eine bereichsbezogene Sicherheitsrichtlinie seien für alle von der IT-Leitstelle betreuten PC konkrete Maßnahmen unter „Safe-Guard" realisiert worden.
- Zum zentralen Rechnerraum sei eine Stahltür eingebaut und für die Aufbewahrung von Datenträgern ein Tresor beschafft worden.

Als **allgemeine Erkenntnis** läßt sich aus der Prüfung bereits jetzt folgendes ableiten:

- Die Einbindung einer technikorientierten Dienstleistungseinrichtung in eine bis dahin papierorientierte Verwaltungsorganisation mit einer so heterogenen Aufgabenstellung wie der eines Ministeriums bedarf sehr gründlicher **konzeptioneller, sicherheitstechnischer** und **organisatorischer Vorarbeiten.**
- Wenn zum Zweck der Koordinierung vom Innenministerium bzw. von der IT-Kommission ressortübergreifende, **allgemeinverbindliche Vorgaben** gemacht werden, so sollten diese erkennen lassen, welche Teile als Mindestanforderungen anzusehen sind und welche eher den Charakter von Empfehlungen haben. Die Aktualität dieses Regelwerkes spielt dabei eine besondere Rolle.
- Ist eine bestimmte Vorgehensweise seitens der datenverarbeitenden Stelle für erforderlich und angemessen befunden worden, muß gewährleistet sein, daß diese **Soll-Regelung** auch **in die Praxis umgesetzt** wird. Abweichungen vom „rechten Weg" können nur von demjenigen genehmigt werden, der die Soll-Regelung in Kraft gesetzt hat. Alle anderen Abweichungen müssen als unzulässig angesehen werden.
- Die Dienstleistungsfunktion und der **Verantwortungsbereich** der **IT-Leitstelle** muß **eindeutig definiert** sein. Sie darf sich den verfahrensverantwortlichen Fachabteilungen nicht als unkontrollierbare „black box" darstellen.
- Die **personelle Besetzung** der IT-Leitstelle muß es ihr ermöglichen, die übertragenen Aufgaben auch tatsächlich zu bewältigen. Es muß nicht nur ihr Recht, sondern ihre Pflicht sein, neue Aufgaben erst dann anzunehmen, wenn die bestehenden unter rechtlichen und sicherheitstechnischen Aspekten ordnungsgemäß abgewickelt sind.
- Deshalb dürfen **Sicherheitsrisiken**, die aufgrund personeller oder finanzieller Engpässe entstehen, weder der „Spitze des Hauses" noch den Fachabteilungen verborgen bleiben. Sie haben im Gegenteil hierfür die Verantwortung zu übernehmen.

6.3 Mindestanforderungen an den Grundschutz für IT-Systeme

Eine Checkliste der IT-Kommission legt Mindestanforderungen für durchschnittliche Arbeitsplätze in der Verwaltung fest, an denen mit IT-Systemen gearbeitet wird.

In den vergangenen Jahren sind wir von den datenverarbeitenden Stellen immer wieder aufgefordert worden, die von uns bei Prüfungen benutzten **Checklisten** mit Kriterien für die **Sicherheit von IT-Systemen** zu veröffentlichen. Zur Begründung wurde angeführt, die Behörden hätten dadurch eine Richtschnur zur Beantwortung der Frage: „Haben wir genug in Datensicherheit investiert oder wird der Datenschutzbeauftragte bei einer Überprüfung Anlaß zu Beanstandungen haben?". Wir sind dem Drängen aus mehreren Gründen bisher nicht gefolgt:

- Wir verfügen nicht über eine einheitliche und umfassende Checkliste, sondern „nur" über vielfältige Materialsammlungen, die bei der Vorbereitung von Prüfungen ausgewertet werden.
- Es ist nicht möglich, alle denkbaren automatisierten Verfahren „über einen Leisten" zu schlagen. Die Gefahr, in dem einen Fall über das Ziel hinaus zu schießen, ist ebenso groß, wie das Risiko, in dem anderen Fall bei der Benutzung der gleichen Checkliste spezifische Sicherheitsrisiken nicht zu erfassen.
- Nicht zuletzt erschien es uns auch nicht sinnvoll, für die datenverarbeitenden Stellen „berechenbar" zu werden.

Das Inkrafttreten der **Datenschutzverordnung** (vgl. Tz. 6.1) mit der bindenden Verpflichtung, für alle automatisierten Verfahren **Sicherheitskonzepte** zu entwickeln und umzusetzen, hat die Diskussion um Checklisten erneut angefacht. Ein „Entscheidungsträger" hat das Problem mit folgender Frage auf den Punkt gebracht: „Wenn meine EDV-Abteilung mir den Entwurf eines Sicherheitskonzeptes zur Entscheidung vorlegt, gegen welchen Maßstab soll ich ihn abgleichen? Die Gesetz- und Verordnungstexte sind viel zu abstrakt, um daraus abzuleiten, was im konkreten Fall „erforderlich und angemessen" ist.

Vor diesem Hintergrund haben wir dem Wunsch der IT-Kommission des Landes entsprochen, an der Entwicklung einer Checkliste mit dem Titel **„Mindestanforderungen an den Grundschutz für Standard-IT-Systeme"** mitzuwirken. Von besonderem Interesse war dabei, wie die beiden Begriffe „Grundschutz" und „Standard-IT-Systeme" definiert werden konnten, um eine große, aber nicht zu große Anwendungsbreite für dieses Arbeitsmittel zu erreichen.

Der **Versuch** scheint **gelungen**, weil folgende **Rahmenbedingungen** eingehalten worden sind:

- Es wird ausgegangen von der Verarbeitung von Daten im Rahmen eines **typischen Verwaltungsverfahrens.** Gemeint ist also Verwaltungshandeln, das aktenmäßig zu dokumentieren ist und in der Regel in einen Verwaltungsakt einmündet, in dem zwar personenbezogene Daten verarbeitet werden, die Daten jedoch keinen besonderen Sicherheitsanforderungen unterliegen.

- Für die Verarbeitung von Daten, die einem **besonderen Berufs- oder Amtsgeheimnis** unterliegen, für Verschlußsachen, Personalvorgänge oder Abläufe in den Sicherheitsbehörden ist in der Regel ein höherer Maßstab anzulegen als in der Checkliste definiert.
- Die Checkliste ist anwendbar für **Standard-Arbeitsplätze** wie z.B. vernetzte und unvernetzte PC sowie für übergeordnete Systeme wie z.B. Abteilungsrechner und Server.
- **Gewährleistet** werden soll
  - o die **Verfügbarkeit** der Systeme (z.B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
  - o die **Integrität** der Software und der Daten (z.B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien),
  - o die **Vertraulichkeit** von Daten (z.B. Schutz vor unbefugter Kenntnisnahme von Dateiinhalten, Diebstahl von Datenträgern).
- Die **Rechtmäßigkeit** der Datenverarbeitung und die Einhaltung verfahrensspezifischer Pflichten (Mitbestimmung, Meldepflichten, spezielle datenschutzrechtliche Pflichten etc.) sowie die ergonomischen Erfordernisse können nicht mittels der Checkliste überprüft werden.
- Die Positionen der Checkliste repräsentieren im einzelnen und in ihrer Gesamtheit **Mindestanforderungen** in dem Sinne, daß ein Begründungszwang ausgelöst wird, wenn im Einzelfall eine Anforderung nicht erfüllt wird.
- Die Checkliste soll die **IT-Verantwortlichen** unterstützen, bei der Beschaffung von neuen IT-Systemen Mindestanforderungen zu formulieren. Sie kann auch bei bereits installierten Systemen zur qualitativen Überprüfung von realisierten Maßnahmen dienen.
- Sie ist nicht primär unter datenschutzrechtlichen Aspekten entwickelt worden, sondern unter Berücksichtigung **allgemeiner** (teilweise weitergehender) **Sicherheitsüberlegungen**. Gleichwohl kann sie aber auch bei der Erstellung von datenschutzrechtlichen Sicherheitskonzepten behilflich sein.

Die Checkliste besteht aus nur ca. 30 Einzelpositionen. Das ist im Verhältnis zu anderen in der Fachliteratur veröffentlichten Konzepten dieser Art recht „dünn". Gleichwohl wären wir froh, den von der IT-Kommission definierten Standard bei unseren Prüfungen vor Ort regelmäßig vorzufinden. Die Anzahl der Beanstandungen wegen struktureller Sicherheitsmängel würde sich schlagartig reduzieren. Den Entscheidungsträgern in den Behörden ist diese Ausarbeitung deshalb als „Pflichtlektüre" zu empfehlen.

6.4 Sicherheitsvorkehrungen bei der Wartung von Computern

Die Dezentralisierung der Datenverarbeitung läßt den Markt für Fernwartung blühen. Behörden müssen beim Abschluß von Wartungsverträgen Schutzvorkehrungen treffen.

Durch die derzeitige Wandlung der EDV-Konzeptionen weg von der zentralisierten Verarbeitung in Rechenzentren (z.B. in der Datenzentrale) hin zu **dezentralen Einzelplatzlösungen** oder **lokalen Netzwerken** (Schlagwort: „Jeder Abteilung ihren Rechner") erhält die Problematik der **Wartung** dieser technischen Systeme durch Dienstleister aus datenschutzrechtlicher Sicht ein neues Gewicht. Die regelmäßigen (präventiven) Wartungszyklen zu festen Zeiten in großen Rechenzentren lassen sich technisch und organisatorisch leichter in den Griff bekommen, als die neuerdings übliche Ad-hoc-Wartung nach Eintritt von Defekten oder Softwarefehlern.

Außerdem ist festzustellen, daß viele Behörden noch nicht über hinreichende Erfahrungen bezüglich der **Ausgestaltung von Wartungsverträgen** verfügen, insbesondere wenn es sich um die Vereinbarung von Fernwartung handelt. Die einschlägigen datenschutzrechtlichen Bestimmungen legen folgende Anforderungen an die vertraglichen Vereinbarungen fest:

- **Auftragnehmer** sind unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der technischen und organisatorischen Sicherungsmaßnahmen **sorgfältig auszuwählen**.
- **Aufträge** und ergänzende Weisungen sind **schriftlich** festzulegen.
- Die erhöhten Anforderungen der Verarbeitung von Daten, die einem **besonderen Berufs- oder Amtsgeheimnis** unterliegen, sind zu beachten.
- Es ist eine Verfahrensweise zu vereinbaren, die gewährleistet, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den **Weisungen des Auftraggebers** verarbeitet werden.
- Die Zulässigkeit von **Unterauftragsverhältnissen** und die Kontrollkompetenzen sind schriftlich festzulegen.

Dies alles ist für kleinere und mittlere Behörden nicht ganz einfach in die Praxis umzusetzen. Deshalb haben wir den datenverarbeitenden Stellen im Lande in einem **15-Punkte-Katalog**, der im **Amtsblatt** (Amtsbl. Schl-H. 1994, S. 140) veröffentlicht worden ist, dargestellt, welche praktischen Konsequenzen sich aus den jeweiligen gesetzlichen Regelungen ergeben. Diese Empfehlungen sollten als **Checkliste** benutzt werden. Nur wenn alle Punkte mit einem „Okay" versehen werden können, darf der Behördenleiter hinreichend sicher sein, daß unbefugte (in der Regel fahrlässige) Modifikationen an Hardware, Software und Daten durch den Dienstleister

nicht zu befürchten sind. Anderenfalls sind Erörterungen mit dem Anbieter von Fernwartungsdienstleistungen und ggf. Beratungsgespräche mit uns angezeigt.

7. Neue Medien und Technologien

7.1 Telefonieren in Europa – Wirtschaftlichkeit vor Sicherheit?

Neue Technik im Bereich der Telekommunikation bringt neue Gefahren für die Kommunikationsfreiheit. Ein Richtlinienentwurf der Europäischen Union, der dem entgegenwirken soll, ist in den vergangenen Jahren mehrfach verwässert worden.

„Telefonieren ist auch nicht mehr das, was es einmal war." Diese auf den ersten Blick banale Feststellung kann man bei näherem Betrachten in vielfältiger Hinsicht wörtlich nehmen:

- Statt der Handvermittlung bzw. der mechanischen Relais stellen Computer die Verbindungen her.
- Unsere Sprache ist nicht mehr das einzige, was wir per Telefon jemandem anderen übermitteln können. Bilder, Texte, ja ganze Dateien werden von den neuen Techniken digitalisiert bewältigt.
- Aus den Telefonapparaten sind multifunktionale Kommunikationsterminals geworden.
- Man hat es nicht mehr ausschließlich mit „der Post" und ihren Beamten zu tun, sondern auch mit Privatunternehmen und Verkäufern, die eine Unzahl spezieller Dienstleistungen anbieten.
- Man braucht zwar keine Leitung mehr zum Telefonieren, kann dafür aber mit Hilfe eines Minicomputers in Form einer Chipkarte „mobil" kommunizieren.
- Das Telefonieren hinterläßt neuerdings Datenspuren in den Computern, die die Kommunikation steuern. Wo welche Daten anfallen, ist von Netz zu Netz und von System zu System unterschiedlich.
- Die Unternehmen, die Telekommunikationsdienstleistungen anbieten, agieren grenzüberschreitend. Wer mit wem zusammen in welchem Land sich wie betätigt, ist nur noch von Fachleuten zu durchschauen.

Angesichts der von allen Teilnehmern am Telefonverkehr verlangten Vertraulichkeit war es nur konsequent, daß die **EG-Kommission** bereits im Jahre 1990 dem Rat der Europäischen Gemeinschaft neben allgemeinen Vorschlägen zu einer EG-Datenschutzrichtlinie auch den Entwurf einer speziellen **„Richtlinie zum Schutz personenbezogener Daten in digitalen Telekommunikationsnetzen, insbesondere ISDN und**

Mobilfunk" vorgelegt hat. Die Regelungen in diesem Entwurf konnten als durchaus datenschutzfreundlich und der deutschen Datenschutzgesetzgebung nicht unähnlich bezeichnet werden:

- Die Verarbeitung der anfallenden personenbezogenen Daten sollte nur für abschließend aufgeführte Telekommunikationszwecke zulässig sein.
- Die Entwicklung von „Teilnehmerprofilen" war untersagt.
- Die Speicherungsdauer von Teilnehmerdaten war an die Dauer des Vertragsverhältnisses geknüpft.
- Gesprächsinhalte sollten nicht gespeichert werden dürfen.
- Den Teilnehmern wurden Auskunfts-, Berichtigungs- und Löschungsansprüche zugestanden.
- Datenübermittlungen sollten von einer gesetzlichen Grundlage bzw. von der Einwilligung der Teilnehmer abhängig sein.

Diese **Grundsätze** wurden in den sich über mehrere Jahre hinziehenden Beratungen in den verschiedenen Gremien der „Eurokratie" sehr stark **verwässert**. Die Richtlinie sollte mit einem Mal nicht mehr primär datenschutzrechtliche, sondern wirtschafts- und industriepolitische Ziele verfolgen. Es gelte auf die unterschiedlichen Datenschutzregelungen in den Mitgliedsstaaten durch eine Harmonisierung des Telekommunikationsrechts zu reagieren. Sie seien ein Hindernis für die Telekommunikationsanwendungen im gemeinsamen Binnenmarkt, weil sie die Erreichung hoher Stückzahlen gleicher Geräte bei der Produktion verhinderten. Dementsprechend liegen nunmehr im letzten Entwurf die Schwerpunkte im technischen Bereich und weniger im Bereich des Schutzes der Teilnehmerrechte. Aber selbst damit ist die Lobby der Telekommunikationsunternehmen offenbar noch nicht zufrieden. Sie fordert noch weitergehende „Liberalisierungen".

Dem treten die **Datenschutzbeauftragten** des Bundes und der Länder entgegen. Sie begrüßen zwar, daß die Europäische Kommission mit der neuen Vorlage ihre Absicht bekundet hat, insoweit bereichsspezifische Regelungen zu schaffen, und fordern auch eine zügige Verabschiedung. Gleichzeitig plädieren sie aber für die Rücknahme der Aufweichungen. In diesem Zusammenhang stellen sie u.a. folgende **Forderungen**, die ihres Erachtens zur **Gewährleistung der Vertraulichkeit** der Kommunikation in der Europäischen Union realisiert werden müßten:

- Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Eine Zweckentfremdung der sensiblen Kommunikationsdaten schon bei „berechtigten Interessen" der Verarbeiter ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung.

- Auch das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.
- Die Speicherung von Kommunikationsinhalten nach Beendigung der Übertragung sollte – wie im ursprünglichen Richtlinienentwurf vorgesehen – untersagt werden.
- Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte – wie es der ursprüngliche Richtlinienentwurf ebenfalls vorsah – auf Unionsebene garantiert werden.
- Den angerufenen Teilnehmern sollte die Aufnahme ihrer Rufnummer in Einzelgebührennachweise der Anrufer freigestellt werden. Soweit dies nicht möglich ist, sollte zumindest die ursprünglich vorgesehene Verkürzung der Zielnummer um die letzten vier Ziffern vorgeschrieben werden.

Gewiß keine extremen Forderungen. Uns ist gleichwohl bewußt, wie schwierig es werden wird, auf europäischer Ebene das Ergebnis vierjähriger Einflußnahme „interessierter Kreise" wieder auszugleichen. An diesem Beispiel wird sich zeigen, ob es den Datenschutzbeauftragten der einzelnen Bundesländer in Zukunft noch möglich sein wird, Einfluß zu nehmen auf Entscheidungen der europäischen Union, die wesentliche Auswirkungen haben auf die von ihnen zu schützenden Rechte der Bürger, z.B. derjenigen zwischen Nord- und Ostsee.

7.2 Chipkarten – die nächste Computergeneration

Nach der massenhaften Einführung von PC steht die nächste Computergeneration ins Haus: Chipkarten. Ihr Einsatz birgt neuartige Risiken und ist nur bei Implementierung einer anspruchsvollen Sicherheitstechnik vertretbar.

Als die Datenzentrale Schleswig-Holstein im Jahre 1968 ihren ersten Computer in Betrieb nahm, mußten Räume von ca. 100 qm Größe mit einem Doppelboden und einer Klimaanlage besonders hergerichtet werden. Wegen der installierten Millionenwerte bestanden die Fenster aus Sicherheitsglas, die Eingänge waren bewacht. Selbst für die Profis war zu jener Zeit unvorstellbar, daß 25 Jahre später die gleiche Rechenleistung von dem Kaufhaus-PC erbracht werden könnte. Heute lächeln viele Datenverarbeiter über ihre Kollegen von damals, ohne zu realisieren, daß der **nächste** große **Schritt** der **Computerrevolution** bereits vollzogen ist. Weil es die Grenzen ihres Vorstellungsmögens sprengt, haben viele die Rechner des kommenden vierten Jahrzehnts der Computerentwicklung noch nicht einmal als solche erkannt, obwohl ihre Prototypen gerade in einer Stückzahl von 72 Millionen in die Briefkästen gesteckt worden sind (vgl. Tz. 4.8.1).

Die Rede ist von **Prozessorchipkarten**. Ein Stück dünnen Plastiks mit den Außenabmessungen von 8,5 x 5,5 Zentimeter, auf denen sich ein goldfarbener Fleck in der Größe von 25 Quadratmillimetern befindet.

Dahinter verbirgt sich ein Computer, der zur Zeit den Inhalt einer ganzen Tageszeitung speichern und eine Million Befehle in der Sekunde abarbeiten kann. In wenigen Jahren werden Prozessorchips auf dem Markt sein, die das Speichervolumen von 10.000 eng beschriebenen Schreibmaschinenseiten haben und 10 Millionen Instruktionen in der Sekunde abarbeiten können.

Warum sieht die **neue Computergeneration** aber so anders aus, als die „Mainfraimes" in den Großrechenzentren, die „PC" auf den Schreibtischen in den Büros und die „Laptops" auf den Knien der Studenten? Weil die Konstrukteure zu folgenden Erkenntnissen gekommen sind:

- Die Tastaturen, die Bildschirme und die Drucker lassen sich auch künftig nicht wesentlich verkleinern, da sonst die Bedienungsfreundlichkeit bzw. die Funktionalität leidet.
- Die Technik dieser drei Elemente ist andererseits so weit standardisiert, daß sie praktisch überall verfügbar ist bzw. zur Verfügung gestellt werden kann. Ihre Benutzung muß keinerlei Restriktionen unterliegen (vergleichbar den öffentlichen bzw. frei zugänglichen Telefonen, Kopiergeräten, Blutdruckmeßgeräten usw.).
- Von Fall zu Fall unterschiedlich sind in der Regel also nur die Anwendungssoftware und die Daten der Computersysteme, denn bereits auf der Ebene der Betriebssysteme bestehen Industriestandards.
- Trennt man diese Standardkomponenten von den individuellen Elementen ab, bleibt ein Computer im Scheckkartenformat übrig.
- Um ihn in Betrieb zu setzen, braucht man ihn nur in einen Adapter zu stecken, der die Verbindung zu den Ein- und Ausgabekomponenten herstellt. Bei kontaktlosen Anwendungen entfällt sogar dies.
- Um die Akzeptanz/Nutzbarkeit dieser Computer zu gewährleisten, muß man nur Schreib- und Lesestationen in genügender Anzahl zur Verfügung stellen.

Die wirtschaftlich interessanten **Anwendungsgebiete** für diese Minis scheinen grenzenlos:

- Die Telekom ist mit ihren Telefonkarten überaus erfolgreich. Ca. 150 Millionen Exemplare sorgen dafür, daß das Knacken von Münztelefonen zunehmend unattraktiv wird und die Post in Höhe der noch nicht vertelefonierten Einheiten einen zinslosen Kredit erhält. Die wiederaufladbare Karte steht vor der Tür.
- Auf die Krankenversicherungskarten wurde bereits unter Tz. 4.8.1 eingegangen.

- Die Patientenchipkarte enthält das Ergebnis der bisherigen ärztlichen Behandlungen und den medizinischen Status des Inhabers. Bei einem Unfall prüft der Arzt möglicherweise bald nicht mehr zuerst den Puls, sondern sucht nach der Chipkarte.
- Mittels „Electronic-Cash" soll dem Bargeld der Garaus gemacht werden. Man geht zur „Geldtankstelle", um den Chip wieder zu „füllen".
- Mit der gleichen Karte bezahlt man die Benutzung der öffentlichen Verkehrsmittel. Damit das ganz schnell geht, wird „kontaktlos" gewissermaßen im Vorübergehen gelesen.
- Chipkarten sollen zur Verschlüsselung von Nachrichten dienen.
- Am Arbeitsplatz wird die geleistete Arbeit genauso abgerechnet wie der Verzehr des Brötchens in der Kantine.

Prognose eines Entwicklungsingenieurs: „Die Chipkarte wird unsere Lebensgewohnheiten total verändern".

Für den Landesbeauftragten für den Datenschutz, dessen gesetzlicher Auftrag auch die Beratung des Parlaments und der Verwaltung über die **Sozialverträglichkeit** neuer Datenverarbeitungstechniken umfaßt, ergeben sich aus dieser Entwicklung eine Vielzahl von Problemstellungen. Einige Gründe:

- In dem Moment, in dem ein Bürger seine Chipkarte in das Ein-/Ausgabegerät einer anderen Person bzw. Institution steckt, gibt er zumindest vorübergehend die Verfügungsgewalt über „seinen Computer" auf. Dies ist eine völlig neue Situation. Sie ist vergleichbar mit der Hingabe einer Geldbörse mit dem Bemerken: „Ich will den Betrag von 45,70 DM bezahlen, nehmen Sie ihn bitte heraus". Ohne **wirksame Sicherungsmechanismen** wird ein solches Verfahren nicht verantwortbar sein.
- Weder die gespeicherten Datenbestände noch die Programme sind für den Eigentümer der Chipkarte ohne besondere Hilfsmittel (Computer und Programme) lesbar. Diese Programme können jedoch nicht von ihm selbst erstellt werden. Ein Vergleich drängt sich auf: Ein **Analphabet** besitzt ein Buch, um seinen Inhalt zu erfassen, braucht er einen Vorleser.
- Den Computer auf der Chipkarte werden die meisten Eigentümer nicht selbst programmieren können. Die Software wird ihnen also just von demjenigen zur Verfügung gestellt, der auch ein wirtschaftliches Interesse an den anschließend gespeicherten Daten hat. Wie kann der **Betroffene überprüfen**, daß tatsächlich nur die Funktionen ausgeführt und Daten gespeichert werden, die zwischen ihm und dem Kartenherausgeber vereinbart worden sind?
- Welche Teile der Verarbeitungslogik sich auf dem Prozessorchip befinden und welche in dem Ein-/Ausgabegerät, ist technisch gesehen frei wählbar. Wie kann verhindert wer-

den, daß durch **manipulierte Programme** in diesen Geräten Speicherungen auf der Chipkarte vorgenommen werden können, die von dem eigenen bzw. von den Standardlesegeräten gar nicht als solche erkannt werden können?

- Der Traum aller Chipkartenentwickler ist die multifunktionale Karte, auf der sich mehrere voneinander abgeschottete Datenbestände befinden. Wie gut müssen dann die **Abschottungsmechanismen sein**, um zu verhindern, daß beim legalen Lesen eines Teilbereiches der gespeicherten Daten Gesamtkopien des Chipkarteninhaltes gemacht werden, um dann später „im stillen Kämmerlein" die Sicherheitsmechanismen zu knacken.
- Bisher ist es den Steuerpflichtigen, den Bankkunden oder den Patienten relativ gleichgültig, ob die Daten in den Computern der Finanzämter, Banken oder Kliniken richtig sind. Sie verlassen sich auf die **Authentizität** der Steuerbescheide, Kontoauszüge oder Patientenakten. Wird man auch in Zukunft von dieser Annahme ausgehen können? Wann wird der Inhalt des Chips zum **„Original"** und das papierene Dokument zur **Kopie**? Die rechtlichen Konsequenzen dürften „revolutionär" sein.

Die vorstehenden Beispiele können um eine Vielzahl weiterer offener Fragen ergänzt werden. Deshalb sehen wir den Trend zu **immer neuen Feldversuchen** mit den Chipkarten (Patientenchipkarte, Apo-Karte, Röntgencard, Telekarte) mit durchaus **„gemischten Gefühlen"**. Die Forderung lautet: „Schluß mit den angeblichen Praxistests, hinter denen in Wahrheit oft nur das Besetzen von Marktpositionen steckt!" Statt dessen sollten **verbindliche Sicherheitsstandards** für die verschiedenen Anwendungsbereiche entwickelt werden, bevor vollendete Tatsachen geschaffen sind. Es wäre fatal, wenn sich bei den Chipkarten das wiederholte, was wir mit den Viren in der PC-Welt derzeit erleben: Wir können auf die PC nicht mehr verzichten, uns gegen Virenschäden aber kaum wirksam schützen.

8. Was es sonst noch zu berichten gibt

8.1 Fehlerhafte Dateimeldungen binden Arbeitskraft

Ein Sachbearbeiter in unserer Dienststelle ist zur Zeit vollauf damit beschäftigt, unvollständige, fehlerhafte oder für Dritte nicht verständliche Meldungen zur Dateienübersicht durch schriftliche oder telefonische Rücksprachen bei den Behörden zu korrigieren. Die mehrseitigen, mit Beispielen versehenen Ausfüllhinweise, die wir im Amtsblatt (Amtsbl. Schl.-H. 1992, S. 674) veröffentlicht haben, sind offenbar von vielen Behörden gar nicht zur Kenntnis genommen worden. Wie sonst könnte man sich erklären, daß als Rechtsgrundlage für Datenspeicherungen z.B. das Grundgesetz angeführt wird oder daß man glaubt, unter der Datenfeldbezeichnung

„CARNOFSCY 9" könne sich jemand etwas vorstellen. Bezeichnend sind auch die Angaben zur Speicherungsdauer wie z.B. „verfügbarer Speicherplatz". Ob unter diesen Umständen die vom Landesdatenschutzgesetz geforderte für jedermann verständliche Dateienübersicht jemals Realität werden kann, muß bezweifelt werden.

8.2 Virenprobleme offenbar größer als zugegeben

Datenverarbeiter sind im allgemeinen nicht gerade öffentlichkeitsscheu. Ihre Erfolge beim Einsatz der Informationstechnik zur Rationalisierung und Qualitätsverbesserung werden in den entsprechenden Publikationen hinreichend gewürdigt. Bei hausgemachten Schwierigkeiten hält man sich jedoch gerne „bedeckt". Das gilt z.B. für das Problem der Computer-Viren. Es wird nach wie vor so wenig über Infektionen (Schadensfälle) bekannt, daß man glauben könnte, man habe inzwischen einen hochwirksamen Impfstoff gefunden. Daß die Praxis ein ganz anderes Bild zeichnet, läßt sich aus den Aktivitäten der Datenzentrale ableiten. Sie wird beim Datenträgeraustausch mit ihren Kunden offenbar so von Viren geplagt, daß sie ihnen kostenlos ein Virensuchprogramm zur Verfügung gestellt hat und zum wiederholten Male in mehrseitigen Abhandlungen Vorschläge zur Datenhygiene macht. Durch Virenschäden werden zwar nur in den seltensten Fällen schutzwürdige Belange der Bürger beeinträchtigt. Gleichwohl ist ein Virenbefall aus datenschutzrechtlicher Sicht ein Indikator für Mängel bei den Datensicherungsmaßnahmen. Da man Computerviren nicht bekommt, sondern sich holt, liegt die Vermutung nahe, daß eine Behörde, die insoweit keine wirksamen Abwehrmaßnahmen ergriffen hat, es auch sonst mit der Datensicherheit nicht so genau nimmt. Nur, man redet halt nicht drüber.

8.3 Vorschläge zur kostengünstigen Vernichtung von Altakten

Als Beispiel für den finanziellen Aufwand, den ein wirksamer Datenschutz (vermeintlich) verursacht, werden oftmals die Kosten für die Altaktenvernichtung genannt. Allerdings geht man dabei von den Entgelten für eine „Luxusentsorgung" mit verschlossenen Aluminiumcontainern auf allen Fluren und regelmäßiger Abfuhr durch den Entsorger aus. Dabei wird dann auch noch übersehen, daß diese Methode für besonders sensible Datenbestände gar nicht geeignet ist, weil der Entsorger bereits vor der Vernichtung die Verfügungsgewalt (Schlüsselgewalt) über die Akten erhält. Deshalb unterbreiten wir den Behörden für diese Fälle folgenden sicheren, trotzdem kostengünstigen Vorschlag: Das zu vernichtende Material wird von der Behörde bis zum Abtransport in einem verschlossenen Raum oder Container zwischengelagert. Ein erneuter Zugriff auf die Unterlagen im Zwischenlager wird nicht zugelassen.

Hat die Menge ein Volumen erreicht, das eine Direktablieferung beim Entsorger rechtfertigt, werden die Unterlagen unter Aufsicht eines Mitarbeiters der datenverarbeitenden Stelle verladen. Er begleitet den Transport. Die sofortige Vernichtung der Unterlagen nach Ankunft beim Entsorger wird von ihm überwacht. Über den Entsorgungsvorgang wird eine Aktennotiz gefertigt. Unseres Wissens bieten die meisten Entsorger eine solche Verfahrensweise an.

8.4 Veröffentlichung behördlicher Telefonverzeichnisse als Postwurfsendung

Im Bemühen um eine bürgerfreundliche Verwaltung gehen immer mehr Behörden dazu über, ihr Telefonverzeichnis zu veröffentlichen. Es enthält in der Regel neben den Namen und Telefonnummern der Mitarbeiter auch Angaben über deren Funktion innerhalb der Verwaltung.

Gegen eine solche Veröffentlichung bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Die Mitarbeiter sind hier nicht in ihrer Eigenschaft als natürliche Person und damit als Träger von Grundrechten angesprochen. Sie nehmen vielmehr als Funktionsträger öffentliche Aufgaben für die Behörde wahr. Erst wenn über eine bloße Darstellung behördlicher Tätigkeit hinaus die dienstrechtliche Bewertung eines persönlich zurechenbaren Verwaltungshandelns erfolgt (z.B. im Rahmen eines Disziplinarverfahrens), ist der Mitarbeiter als natürliche Person angesprochen, der Datenschutzrechte für sich in Anspruch nehmen kann. Diese Schwelle wird bei der Veröffentlichung eines Telefonverzeichnisses nicht überschritten.

8.5 Alle Eigentümer in einem Baugebiet sollten einander kennen – oder nicht?

Werden Grundstücksgrenzen neu vermessen, so wird darüber eine „Abmarkungsmitteilung" für den Eigentümer erstellt und als Anlage ein „Grenzprotokoll" beigefügt, aus dem alle betroffenen Grundstücke und die beteiligten Eigentümer hervorgehen. Dies war bislang auch in Schleswig-Holstein Praxis.

Ein Petent war nicht damit einverstanden, daß auf diesem Wege allen an der Vermessung eines größeren Neubaugebietes beteiligten Grundstückseigentümern auch die Eigentumsverhältnisse an seinem Grundstück bekannt werden sollten. Wir haben in Verhandlungen mit dem Innenminister erreicht, daß künftig bei Zusendung der Unterlagen Grundstückseigentümern nur die Namen derjenigen anderen Eigentümer bekannt gegeben werden, mit denen sie eine gemeinsame Grundstücksgrenze haben. Im Grenzprotokoll werden die anderen Grundstücke nur durch Numerierung und nicht mehr durch Benennung des Eigentümers gekennzeichnet.

8.6 Veröffentlichung von Prüfungsberichten der Rechnungsprüfungsämter

Die Gemeindeordnung ist mit dem Ziel geändert worden, daß Schlußberichte über Rechnungsprüfungen der Rechnungsprüfungsämter künftig öffentlich auszulegen sind. Eine größere Transparenz kommunaler Verwaltungstätigkeit sollte so erreicht werden. Wir wiesen in den Beratungen darauf hin, daß solche Berichte zwar in der Regel nur Informationen über die Verwaltung und ihre Funktionsträger enthalten und insoweit datenschutzrechtlich unbedenklich sind. Allerdings kann nicht ausgeschlossen werden, daß sie auch schutzbedürftige Informationen über Einzelpersonen enthalten. Solche Daten sollten nicht öffentlich einzusehen sein. Der Landtag ist unserem Vorschlag gefolgt. Er hat die Veröffentlichung ausgeschlossen, soweit „... schutzwürdige Interessen einzelner entgegenstehen." Die Änderung ist inzwischen in Kraft getreten.

8.7 Verabschiedung eines Gleichstellungsgesetzes

Ein zentraler Punkt in dem vom Landtag verabschiedeten Gleichstellungsgesetz war aus unserer Sicht die für die Gleichstellungsbeauftragten vorgesehene Befugnis, ggf. auch gegen den Willen von Betroffenen in deren Personalakte Einsicht zu nehmen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Bei konsequenter Anwendung dieser Regelung dürfte eine solche Einsichtnahme in der Praxis kaum Bedeutung erlangen. Durch das Wort „soweit" wird dem Dienstherrn die Pflicht auferlegt, im Einzelfall zu prüfen, ob eine die Betroffenen weniger belastende Form der Unterrichtung der Gleichstellungsbeauftragten, insbesondere die Erteilung von Auskünften aus der Personalakte, möglich ist. Aus unserer Beratungs- und Prüfungstätigkeit ist uns bisher kein Fall bekannt geworden, in dem über die bloße Weitergabe der erforderlichen Personaldaten hinaus eine Einsichtnahme in die vollständige Personalakte tatsächlich notwendig gewesen wäre, um eine ordnungsgemäße Aufgabenerfüllung für die Gleichstellungsbeauftragten zu gewährleisten.

Unserer Empfehlung, das Informationszugangsrecht der Gleichstellungsbeauftragten der Regelung für Personalräte nachzubilden, ist der Landtag leider nicht gefolgt.

8.8 Ermächtigung zur Sektenbeobachtung im Landesdatenschutzgesetz

Die Absicht der Landesregierung, eine Dokumentationsstelle für Aktivitäten von Sekten und sektenähnlichen Vereinigungen einzurichten, wurde in dem Moment datenschutzrelevant, als deutlich wurde, daß sie auch personenbezogene Daten verarbeiten soll. Aus diesem Grund wurde § 29 a in das LDSG eingefügt.

Die Regelung stellt klar, daß die Rechte der Sekte selbst und des einzelnen Sektenmitglieds dann zurücktreten müssen, wenn aufgrund konkreter Tatsachen zu befürchten ist, daß von ihrer Tätigkeit Gefahren für das Recht auf Leben, Gesundheit, Eigentum, Persönlichkeitsentfaltung und Menschenwürde, ausgehen.

Zweck der Dokumentation ist die Aufklärung und Warnung einzelner Bürger und von Gruppen, die mit solchen Sekten, Vereinigungen oder von ihnen beherrschten Institutionen in Kontakt kommen.

Die Dokumentationsstelle soll dazu öffentlich zugängliche bzw. bei öffentlichen Stellen vorhandene Informationen erheben, dokumentieren und über sie informieren. Besondere Verwendungsregeln für Daten, wie etwa im Sozialgesetzbuch, stehen einer Weitergabe von Informationen an die Dokumentationsstelle entgegen. Das gleiche gilt auch für solche Daten, die einem besonderen Amts- oder Berufsgeheimnis unterliegen. Eine regelmäßige Aussonderung entbehrlicher Daten und eine Begrenzung des Empfängerkreises von Informationen runden die datenschutzrechtliche Einbindung dieser Dokumentationsstelle ab, die mittlerweile durch Bekanntmachung der Ministerpräsidentin vom 14.11.1994 errichtet worden ist. An der Entwicklung eines Datenschutzkonzepts für die Dokumentationsstelle sollen wir beteiligt werden.

8.9 Dokumentation von Übermittlungsersuchen der Verfassungsschutzbehörden an die Staatsanwaltschaft

Das Landesdatenschutzgesetz verlangt grundsätzlich die Dokumentation von Datenübermittlungen, so daß der Betroffene auch darüber Auskunft erhalten kann.

Bei staatsanwaltschaftlichen Ermittlungsakten ist die Besonderheit zu beachten, daß ihr Inhalt aufgrund der Einsichtnahmerechte auch Dritten zugänglich gemacht werden kann. Dazu zählen nicht nur Behörden, sondern auch Kranken- und Sachversicherungen sowie die Vertreter von Nebenklägern. Sie würden bei einer Einsichtnahme erfahren, daß sich für den Betreffenden auch der Verfassungsschutz „interessiert" hat. Um dies zu verhindern, werden entsprechende Anfragen künftig nicht mehr in der Ermittlungsakte, sondern in den Handakten der Staatsanwaltschaft, die Dritten nicht zur Einsicht zur Verfügung stehen, dokumentiert. Dem Betroffenen muß der entsprechende Schriftverkehr jedoch bei Einsichtnahme in die Akte zugänglich gemacht werden.

8.10 Forschungsprojekt „Gläserne Schule"

Von dem Forschungsprojekt zur Suchtvorbeugung mit der Bezeichnung „Gläserne Schule" erhielten wir durch Zufall

Kenntnis. Auf unsere Nachfragen teilte uns die Koordinierungsstelle schulische Suchtvorbeugung (KOSS) mit, daß es sich um ein schulbegleitendes Projekt handele, an dem sich viele unterschiedliche Schulen in Schleswig-Holstein beteiligten und das im Auftrage des Instituts für Praxis und Theorie in der Schule (IPTS) durchgeführt werde. Sein Ziel sei es, mit Hilfe eines Fragebogens u.a. das Freizeitverhalten von Schülerinnen und Schülern zu untersuchen, um hieraus schulbezogen aber ohne Personenbezug Erkenntnisse für die schulische Suchtprävention zu erlangen.

Die Schülerinnen und Schüler werden zu Kindheit und Familie, Schule, Wohnsituation, Freizeit, Tabakkonsum, Trinkgewohnheiten, nach dem Gebrauch legaler Rauschmittel und zu ihrer Gesundheit befragt. Keine Frage, daß auf diesem Wege ein sensibles Datenprofil entsteht. Deshalb haben wir der Anonymisierung besondere Aufmerksamkeit gewidmet. Sie wird unserer Feststellung nach dadurch erreicht, daß

- Schülerinnen und Schüler die Bögen ohne Identifizierungsmerkmale unbeobachtet ausfüllen,
- die Bögen in verschlossenen und nicht gekennzeichneten Umschlägen unverzüglich zu dem auswertenden Institut der Universität transportiert werden.

Die statistische Aufbereitung, die an die Schulen als Balkendiagramm zurückgeliefert wird, läßt eine Zuordnung der Ergebnisse nur bis zur Klassenstufe zu. Datenschutzverstöße können bei diesem Verfahren vermieden werden.

9. Rückblick

9.1 Protokollierung der Grundbucheinsicht realisiert

In der Vergangenheit hatten wir uns immer wieder dafür eingesetzt, daß schriftlich festgehalten wird, wer aus welchem Grunde in das Grundbuch Einsicht genommen hat. Dem hat der Justizminister nunmehr entsprochen und durch eine Verwaltungsanweisung geregelt, daß jede Einsichtnahme in das Grundbuch protokolliert wird. Damit übernimmt Schleswig-Holstein in dieser Hinsicht eine Vorreiterrolle unter den Bundesländern.

9.2 Verbesserung der Kapazitätsverordnung des juristischen Vorbereitungsdienstes

Im Jahre 1993 (15. TB, S. 22 ff.) berichteten wir, daß bei den Bewerbungen von Rechtskandidaten für den juristischen Vorbereitungsdienst zu viele Personalunterlagen verlangt würden. Wir hielten unter datenschutzrechtlichen Gesichtspunkten die Anforderungen der zugrundeliegenden Verordnung für unverhältnismäßig und regten entsprechende Änderungen an.

Nicht zuletzt deshalb wurde die Kapazitätsverordnung mit unserer Beteiligung im März 1994 novelliert. Auf eine Reihe von Unterlagen wird seither generell verzichtet. Andere werden erst später, im Falle der Einstellung in den Vorbereitungsdienst, gefordert. Auch die ergänzende Verfügung des Oberlandesgerichtspräsidenten als datenverarbeitende Stelle wird die Vorlage nur solcher Unterlagen für die Einstellung der ausgewählten Referendarinnen und Referendare festlegen, die aufgrund beamtenrechtlicher Regelungen erforderlich sind. Die schnelle und angemessene Reaktion auf unsere Prüfung ist für uns ein positives Beispiel für den Umgang mit unseren Prüfergebnissen.

9.3 Neue Richtlinien sollen den Anspruch schwangerer Frauen auf anonyme Beratung sicherstellen

Im 16. Tätigkeitsbericht (S. 58) hatten wir über die Vorschläge berichtet, die wir zur Sicherstellung des Datenschutzes bei der Beratung vor einem Schwangerschaftsabbruch der Sozialministerin gegenüber geäußert hatten. Diese haben nunmehr ihren Niederschlag in den vorläufigen Richtlinien über die Anerkennung der entsprechenden Beratungsstellen gefunden:

- Alle Ratsuchenden sind vor Beginn der Beratung darauf hinzuweisen, daß sie sich anonym beraten lassen können.
- Der beratenden Person braucht die ratsuchende Schwangere zu keinem Zeitpunkt ihren Namen zu nennen. Auch unabhängig von der Angabe des Namens ist die beratende Person zur Verschwiegenheit verpflichtet.
- Die beratende Person vergibt für jede Ratsuchende eine Beratungsnummer. Diese Nummer wird für das Protokoll, das anonym geführt wird, und ggf. auch für die spätere Bescheinigung über die Beratung verwendet.
- Die Beratungsbescheinigung ist von einer anderen Person als der auszustellen, welche die Beratung durchgeführt hat. Die Beratungsstelle kann jedoch zur Ausstellung der Bescheinigung eine ausreichende Identifizierung der Beratenen verlangen. Vorgelegt zu werden braucht jedoch nur ein Personalausweis oder ein amtliches Dokument auf ihren Namen.
- Das Beratungsprotokoll muß bis zum Ablauf des folgenden Jahres aufbewahrt werden und ist dann zu vernichten. Liegt eine Anerkennung der Beratungsstelle nicht mehr vor, sind alle Unterlagen innerhalb von drei Monaten nach Wegfall der Anerkennung zu vernichten.

9.4 Übermittlung vollständiger Grundstückskaufverträge zur Ausübung des Vorkaufsrechts eingeschränkt

Zur Ausübung des Vorkaufsrechts der Gemeinden hat der Innenminister des Landes Schleswig-Holstein unsere Vor-

schläge aufgegriffen und durch Runderlaß im Juli 1994 nunmehr ein gestuftes Verfahren für die Übersendung von Grundstückskaufverträgen verbindlich vorgeschrieben. Danach erhält die Gemeinde zunächst nur die Information, daß ein bestimmtes Grundstück verkauft worden ist. Erst wenn daraufhin die Entscheidung getroffen wird, daß eine Ausübung des Vorkaufsrechts tatsächlich in Betracht kommt, wird der vollständige Kaufvertrag nachgefordert. Die zur Umsetzung dieses Verfahrens ebenfalls notwendige Unterrichtung der Notare wurde über die Notarkammer veranlaßt.

9.5 Akteneinsichtsrecht in Krankenakten der Psychiatrie durchgesetzt

Im vorangegangenen Tätigkeitsbericht hatten wir über die Probleme eines zwangsweise untergebrachten Patienten berichtet, seine Krankenakten einzusehen (vgl. 16. TB, S. 62).

In dem geschilderten Fall wurde selbst unserer Dienststelle die Akteneinsicht durch die Fachklinik verweigert. Sie konnte erst nach Einschaltung der Ministerin für Arbeit, Soziales, Jugend und Gesundheit 18 Monate nach Eingang der Beschwerde vorgenommen werden.

Die Fachklinik wird dem Petenten nunmehr den weit überwiegenden Teil der Krankengeschichte in Anwesenheit eines Arztes zur Einsichtnahme vorlegen. Wir haben den Petenten darauf hingewiesen, daß er zu diesem Termin einen Arzt seines Vertrauens oder seinen Rechtsanwalt hinzuziehen könne.

9.6 Auskunftserteilung durch den Verfassungsschutz

Als bei der Novellierung des Landesverfassungsschutzgesetzes auch der Auskunftsanspruch der Bürgerinnen und Bürger eingeführt wurde, hatten einige befürchtet, die Behörden würden nach Inkrafttreten solcher Vorschriften von einer ungeheuren Welle an Auskunftsbegehren überschwemmt und an den Rand der Arbeitsunfähigkeit gebracht.

Nichts davon ist eingetreten. Der Verfassungsschutz in Schleswig-Holstein ist seit 1990 insgesamt 74mal um Auskunft gebeten worden. In keinem Fall wurde die Auskunft verweigert. Nur in einem Fall wurde die Auskunft beschränkt. Ansonsten wurden umfassende Auskünfte gegeben.

Die Vorschriften über die Auskunftspflicht der Sicherheitsbehörden haben sich demnach in der Praxis als gelungener Kompromiß zwischen mehr Transparenz für den Bürger einerseits und Erhaltung der Arbeitsfähigkeit der Sicherheitsbehörden andererseits bewährt. Von einer spürbaren Verschlechterung der Sicherheitslage war bislang nicht die Rede.

10. DATENSCHUTZAKADADEMIE

Das Jahresprogramm 1995 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN baut auf den Erfahrungen aus den Veranstaltungen der Jahre 1993/94 auf. Auch die Rückmeldungen der Teilnehmerinnen und Teilnehmer sowie die Ratschläge der Kuratoriumsmitglieder der DATENSCHUTZAKADEMIE wurden berücksichtigt. Es ist ein Programm erarbeitet worden, das die bewährten Grundkurse der DATENSCHUTZAKADEMIE fortführt und um spezielle Veranstaltungen ergänzt. Dies führt zu differenzierten Formen der Wissensvermittlung. Künftig wird zwischen folgenden Veranstaltungstypen unterschieden:

Kurse:

Sie vermitteln fundierte datenschutzrechtliche Kenntnisse. Die Bestimmungen des allgemeinen und bereichsspezifischen Datenverarbeitungs- und Datenschutzrechts werden anhand von praktischen Beispielen erläutert, ausgewählte Sachverhalte werden in Gruppenarbeit datenschutzrechtlich beurteilt. Die Teilnehmer erhalten Skripten, die so aufgebaut sind, daß sie auch als Nachschlagewerk für die praktische Umsetzung der erworbenen Kenntnisse dienen können.

Seminare:

Sie stellen die Verknüpfung der Theorie mit der Praxis in den Vordergrund. Nach einer Einführung in das jeweilige Datenverarbeitungsrecht werden die praktischen Konsequenzen anhand typisierter, gleichwohl konkreter Fälle aus der Prüf- und Beratungspraxis des Datenschutzbeauftragten, (z.T. unter Zugrundelegung bestimmter Hardware-Software- und Datenkonstellationen) aufgezeigt. Die Teilnehmerinnen und Teilnehmer setzen die erworbenen Kenntnisse in „praxisnahen" Übungen um. Die Seminarunterlagen bestehen aus den „Fällen" und den in den Übungen erarbeiteten Ergebnissen.

Workshops:

In den Workshops steht die aktive, praktische Erarbeitung von Problemlösungen im Vordergrund. Angestrebt wird eine möglichst homogene Zusammensetzung des Teilnehmerkreises, damit dessen Interessenslage in die Auswahl und Lösung der „Fälle" eingebracht werden kann. Die zu behandelnden Sachverhalte werden zum großen Teil durch die Teilnehmerinnen und Teilnehmer selbst ausgewählt, die Ergebnisse unter der Anleitung der Referenten von ihnen erarbeitet. Auf diese Weise entstehen unmittelbar in der Praxis verwendbare Unterlagen.

Im übrigen behält die DATENSCHUTZAKADEMIE auch 1995 ihre bisherigen Arbeitsprinzipien bei:

- Zusammenarbeit mit anderen Fortbildungseinrichtungen des Landes, insbesondere mit der Verwaltungsfachhochschule in Altenholz und mit der Verwaltungsschule in Bordesholm,
- Kostendeckung durch die Teilnehmerbeiträge,
- So wenig bürokratischer Aufwand wie möglich, soviel Aktualität und Flexibilität wie mit den vorhandenen Kräften leistbar,
- Offenheit für weitere Veranstaltungen, in denen die speziellen Wünsche der datenverarbeitenden Stellen berücksichtigt werden.

Im einzelnen führt die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN folgende Veranstaltungen durch:

Beauftragte für Sozialdatenschutz	20.-24.02.1995
Datenschutzverordnung des Landes Schl.-Holst.	27.-28.02.1995
Entwicklung eines Datensicherheitskonzeptes für ein Krankenhaus	16.-17.03.1995
Behördliche Datenschutzbeauftragte	27.-31.03.1995
Schutz von Personaldaten	27.-28.04.1995
Mitarbeiter der Sozialämter	08.-10.05.1995
SGB-Änderungsgesetz	10.-12.05.1995
Führung von Personalakten	18.-19.05.1995
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	22.-24.05.1995
Einstieg in das Datenschutzrecht	01.06.1995
Datenschutz im Ordnungsamt	04.-05.09.1995
Datenschutz im Bauamt	05.-06.09.1995
Datenschutz an der Schule	07.-08.09.1995
Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	28.-29.09.1995
Datenverarbeitungsrecht für Führungskräfte in der Verwaltung	04.-06.10.1995
Behördliche Datenschutzbeauftragte	23.-27.10.1995
Revisionsfähigkeit der automatisierten Datenverarbeitung	06.-08.11.1995
Datenschutz im Bereich der Umweltverwaltung	09.-10.11.1995

Das Jahresprogramm kann angefordert werden **beim Landesbeauftragten für den Datenschutz, Düsternbrooker Weg 82, 24105 Kiel.**

Weitergehende Auskünfte zur inhaltlichen Gestaltung der Kurse geben telefonisch:

unter 0431/596-3291 Frau Molt und
unter 0431/596-3281 Frau Harks

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

Datenschutz in Schleswig-Holstein
Text des Landesdatenschutzgesetzes und
des Bundesdatenschutzgesetzes
mit einer erläuternden Einführung

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

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 1995

BfD-INFO 1: Bundesdatenschutzgesetz
Text und Erläuterung

BfD-INFO 2: Der Bürger und seine Daten

BfD-INFO 3: Schutz der Sozialdaten

herausgegeben vom Bundesbeauftragten für den Datenschutz