SCHLESWIG-HOLSTEINISCHER LANDTAG
14. Wahlperiode

Drucksache 14/10
25. 04. 96

Bericht

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

**Achtzehnter Tätigkeitsbericht
(Berichtszeitraum: März 1995 bis Februar 1996)**

In der Anlage übersende ich gemäß § 23 Abs. 3 Satz 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen vom 30. Oktober 1991 den achtzehnten 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, 2300 Kiel 1, Fernruf 04 31/6 20 95, zu beziehen.

Inhaltsverzeichnis **Seite**

1.	**Zur Situation des Datenschutzes in Schleswig-Holstein**	**6**
1.1	Gesetzgebung, Kontrolle, Beratung	6
1.1.1	Gesetzgebung	6
1.1.2	Kontrolle	7
1.1.3	Beratung	11
1.2	Die Ausstattung der Dienststelle	11
2.	**Der Weg in die Computergesellschaft**	**14**
2.1	Grundrechtsfreundliche Technik	14
2.2	Der Große Lauschangriff - was kommt als nächstes?	16
3.	**Datenschutz im Landtag**	**19**
3.1	Informationsrechte des Parlaments und Datenschutz Betroffener	19
3.1.1	Personenbezogene Daten in Antworten auf parlamentarische Anfragen	19
3.1.2	Aktenvorlagebegehren eines Ausschusses und der Schutz von Personaldaten	19
3.1.3	Nachprüfung der Berufung eines Hochschullehrers durch den Landtag	20
3.2	Keine Verwertung von Stasi-Abhörprotokollen durch den „Schubladen-Untersuchungsausschuß“	21
3.3	Datenschutzordnung für den Landtag	22
4.	**Datenschutz in der Verwaltung**	**23**
4.1	Kommunalbereich	23
4.1.1	Ein X für eine Unterschrift	23
4.1.2	Wenn Bürger Behördenfehler ausbaden müssen	24
4.1.3	... das haben wir immer so gemacht	25
4.1.4	Verwaltungsvorschriften für Gewerbeanzeigen verbessert	28
4.1.5	Sitzungsprotokolle auf Diskette?	29
4.1.6	Datenschutz bei Wahlen	30
4.2	Polizei	31
4.2.1	Der lange Schatten der Vergangenheit	31
4.2.2	Belehrung über das Aussageverweigerungsrecht in Vernehmungsbögen fehlerhaft	32
4.2.3	Auskunft durch die Polizei bei laufenden Ermittlungsverfahren	33
4.2.4	Übermittlung von Daten durch die Polizei an den Arbeitgeber einer Zeugin	35
4.2.5	Videoüberwachung erfaßt auch korrekte Autofahrer	36
4.2.6	Fotos vom Beifahrer werden nicht mehr herumgezeigt	37
4.2.7	Speicherung von Daten über Opfer von Straftaten	37
4.2.8	Computergestütztes polizeiliches Arbeitsplatzsystem (COMPAS)	39
4.2.9	EUROPOL: Jeder kann betroffen sein	41
4.2.10	Verfassungsbeschwerde gegen das Verbrechensbekämpfungsgesetz	44

4.3	Verfassungsschutz	45
4.3.1	Übermittlung von Daten zwischen den Verfassungsschutzbehörden	45
4.3.2	Prüfung beim Verfassungsschutz	46
4.4	Justizverwaltung	48
4.4.1	GAST: Abschluß einer unendlichen Geschichte	48
4.4.2	„Ähnlichenservice“ zu Lasten Unbeteiligter	50
4.4.3	Verfahrensakten bei der Justiz nicht immer in besten Händen	51
4.4.4	Kleine Nachlässigkeiten mit großen Wirkungen	52
4.4.5	Ist Post vom Gerichtsvollzieher stets „Verschlußsache“?	53
4.5	Umweltschutz	54
4.5.1	Privatisierung der Abfallentsorgung	54
4.5.2	Wann kommen die Verordnungen im Umweltrecht?	57
4.6	Wirtschaft, Technik und Verkehr	58
4.6.1	Schnelle Reaktion auf unsere Kontrollergebnisse	58
4.6.2	Speicherung personenbezogener Daten aufgrund der Erteilung von Taxenkonzessionen umgehend neu geregelt	58
4.6.3	Bundesgesetzgeber plant weitere Verdatung der Autofahrer	60
4.6.4	Bürgerunfreundlich aus Prinzip?	61
4.7	Sozialwesen	62
4.7.1	Prüfung eines Sozialamtes fördert Umgehung von gesetzlichen Bestimmungen zutage	62
4.7.2	Weitergabe einer Telefonnummer durch das Jugendamt mit fatalen Folgen	63
4.7.3	Unbefugte Übermittlung von Sozialdaten an einen Zahnarzt	64
4.7.4	Hilfeempfänger bloßgestellt	64
4.7.5	Weitergabe von Sozialdaten an Wohnungsbaugesellschaften	65
4.8	Gesundheitswesen	66
4.8.1	Prüfung der Kassenärztlichen Vereinigung Schleswig-Holstein	66
4.8.2	Datenaustausch zwischen Kassenärztlichen Vereinigungen und Krankenkassen im Streit	67
4.8.3	Vergabe von Schreibarbeiten an Externe durch öffentliche Krankenhäuser	69
4.8.4	Chipkarten im Gesundheitswesen	71
4.9	Kultusbereich	73
4.9.1	Automatisiertes Schulverwaltungssystem für die Beruflichen Schulen	73
4.9.2	Kosten für die Datensicherheit treffen Schulträger	74
4.9.3	Datenschutzverordnung zum Schulgesetz läßt nach wie vor auf sich warten	75
4.9.4	Wenn zu Hause ein Schulverwaltungsprogramm mit echten Schülerdaten getestet wird	76
4.9.5	Datenschutz gegenüber Elternvertretern	77

4.9.6	Zuteilung von Kursplätzen an einer Universität durch den Computer	77
4.10	Steuerverwaltung	79
4.10.1	Endlich Regelungen zur Datensicherheit geschaffen	79
4.10.2	Steuerakten von Prominenten gestohlen	80
4.10.3	„Versprochen ist versprochen" gilt auch für die Steuerverwaltung	81
4.10.4	Die Freiheit, zu viel Steuern zu zahlen	83
4.11	Personalwesen	84
4.11.1	Verarbeitung von Bewerberdaten im Polizeibereich neu geregelt	84
4.11.2	Anforderung uneingeschränkter Bundeszentralregisterauskünfte durch die Reaktorsicherheitsbehörde	84
4.11.3	Was nicht in die Personalakte gehört	85
4.11.4	Jährliche Überprüfung des erhöhten Ortszuschlages nicht erforderlich	85
4.11.5	Was darf der Schulelternbeirat über Fehlzeiten der Lehrer erfahren?	86
4.11.6	Neues Personalaktenrecht endlich verabschiedet	87
4.11.7	Aktenordnung für den Personalrat	88
5.	**Datenschutz bei Gerichten**	**89**
5.1	MEGA	89
5.2	Zweckbindung von Daten, die in Prozessen erhoben worden sind	91
6.	**Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung**	**93**
6.1	Erfahrungen mit der neuen Datenschutzverordnung	93
6.2	Sicherheitskonzepte ohne Wenn und Aber	96
6.3	Pilotprojekte - alter Wein in neuen Schläuchen	98
6.4	Computerdiebstahl - ein neues Phänomen	99
6.5	Viren nun auch in Textdokumenten	101
6.6	Was ist Original, was Kopie?	102
6.7	Ergebnisse von Prüfungskontrollen im Bereich der automatisierten Datenverarbeitung	104
6.7.1	Beanstandung akzeptiert ... (3. Auflage)	104
6.7.2	Verbesserungen beim Patientendatenschutz im Lübecker Klinikum - zentrale Probleme aber weiterhin ungelöst	106
6.7.3	Neues Finanzinformationssystem beanstandet	109
6.7.4	Inanspruchnahme externer Dienstleister	112
7.	**Neue Medien und Technologien**	**114**
7.1	Multimedia	114
7.2	Liberalisierung des Telekommunikationsmarktes	117
7.3	Schleswig-Holstein-Netz	119
7.4	Schöne neue ISDN-Welt bei Landtag und Regierung	121
7.5	Elektronische Geldbörsen dürfen keine Datenspuren hinterlassen	123
8.	**Europa**	**125**
8.1	EU-Datenschutzrichtlinie	125
8.2	Entwurf einer Telekommunikationsrichtlinie	127
8.3	Vorbereitung auf Maastricht II	128

9.	**Was es sonst noch zu berichten gibt**	**129**
9.1	Woran der Datenschutz nicht schuld war	129
9.2	Darf die Ehefrau eines Lehrers zu Hause Schulzeugnisse schreiben?	130
9.3	Wenn zwei Polizeibeamte sich streiten	130
10.	**Rückblick**	**131**
10.1	Innenminister sagt ggf. eigene Rechtstatsachensammelstelle für Schleswig-Holstein zu	131
10.2	Asylcard: Pläne noch nicht ad acta gelegt	131
10.3	Denkmalschutzgesetz verabschiedet	131
10.4	Vorerst keine elektronische Autobahnmaut für Pkw	132
10.5	Datenverarbeitung bei der Suchtberatung neu organisiert	132
10.6	Bundesgrenzschutz als verlängerter Arm der Geheimdienste	133
11.	**DATENSCHUTZAKADEMIE**	**134**
	Kurse/Seminare/Workshops 1996	134
12.	**Sommerakademie 1996**	**136**

1. Zur Situation des Datenschutzes in Schleswig-Holstein

1.1 Gesetzgebung, Kontrolle, Beratung

1.1.1 Gesetzgebung

Im vergangenen Jahr hat das Parlament mit der Verabschiedung eines Gesetzes über die staatsanwaltschaftlichen Verfahrensregister (vgl. Tz. 4.4.1) sowie mit der Novelle zum Landesbeamtengesetz (vgl. Tz. 4.11.6) wichtige Lücken in der Datenschutzgesetzgebung des Landes geschlossen. Die ungebrochene Dynamik der Entwicklung und des Einsatzes der elektronischen Datenverarbeitung zwingen aber zu weiteren gesetzgeberischen Anstrengungen. In wichtigen Bereichen sind nach wie vor die Konsequenzen aus dem Volkszählungsurteil zu ziehen.

Das **Landesdatenschutzgesetz** muß innerhalb von drei Jahren an die Vorgaben der EU-Datenschutzrichtlinie angepaßt werden (vgl. Tz. 8.1). In folgenden Bereichen ist die Neugestaltung der derzeitigen Regelungen angezeigt.

- Verbesserung des Schutzes besonders sensibler Daten
- Regelung verbindlicher präventiver Kontrollen bei besonders riskanten Verarbeitungsverfahren
- Einräumung eines Widerspruchsrechts für die Betroffenen unter bestimmten Voraussetzungen
- Verbindliche Einführung behördlicher Datenschutzbeauftragter
- Stärkung der Unabhängigkeit und der Befugnisse des Landesbeauftragten für den Datenschutz
- Entbürokratisierung des Datenschutzes durch Wegfall des zentralen Dateienregisters
- Vereinfachung und Verschlankung der Datenschutzkontrolle durch Zusammenlegung der Kontrolle im öffentlichen Bereich mit der Aufsicht im Privatbereich in einer Hand

Unabhängig vom Anpassungsbedarf an die EU-Richtlinie sollte das LDSG stärker auf neue technische Entwicklungen, etwa im Bereich der Netze und Chipkarten (vgl. Tzn. 7.3 u. 7.5), ausgerichtet werden.

Die Verabschiedung eines **Sicherheitsüberprüfungsgesetzes** ist notwendig, weil die besonders intensive Datenverarbeitung in diesem Bereich nicht mehr länger auf Richtlinien oder den Übergangsbonus ge-

stützt werden kann.

Die tiefgreifenden Veränderungen durch den zunehmenden Computereinsatz in der Medizin sollten dazu führen, daß der Schutz des Patientengeheimnisses gestärkt und in zeitgemäßer Form durch ein **Gesundheitsdatenschutzgesetz** gewährleistet wird (vgl. Tzn. 4.8.4 u. 4.8.2).

Eine Reihe weiterer Gesetze bedarf Korrekturen und Ergänzungen im Hinblick auf die Verarbeitung personenbezogener Daten. Dazu gehören u.a. das Gesetz über Kindertagesstätten, das Vermessungs- und Katastergesetz, das Abfallrecht, das Kommunalabgabengesetz, das Landesmeldegesetz sowie das Rundfunkrecht. In einigen Bereichen steht die Landesregierung in der Pflicht, die vom Gesetzgeber vorgesehenen Rechtsvorschriften zu erlassen (vgl. Tz. 4.5.2).

1.1.2 Kontrolle

Die im Berichtsjahr durchgeführten Kontrollen haben Mängel unterschiedlicher Art zutage gebracht. Es wurden Einzelverstöße, Nachlässigkeiten, Fehlinterpretationen der Gesetze, aber auch Versuche, die Gesetze zu umgehen, und schwere systematische Fehler entdeckt.

Häufig können vermeintlich **kleine Fehler** beim Umgang mit personenbezogenen Daten für die Betroffenen **schwerwiegende Folgen** haben. So mußte eine Petentin ihre Wohnung verlassen und sich wochenlang unter wechselnden Adressen verbergen. Grund: Eine Sozialamtsmitarbeiterin wollte nett sein und gab einem rabiaten Ehemann „nur" die Telefonnummer seiner getrennt lebenden Ehefrau, die gerade einen neuen Unterschlupf gefunden hatte. Hiermit ermittelte er die neue Anschrift, die das Einwohnermeldeamt ihm wegen einer Auskunftssperre verweigert hatte, und bedrohte und drangsalierte die Frau erneut (vgl. Tz. 4.7.2). Ein anderer Petent hatte alle Hände voll zu tun, Forderungen, Mahnbescheide, Versäumnisurteil und Gerichtsvollzieher abzuwehren. Grund: Dem Meldeamt war dreimal nacheinander die gleiche peinliche Verwechslung mit einer anderen Person unterlaufen (vgl. Tz. 4.1.2). Eine Petentin gelangte mit ihrem Geschäftsbetrieb an den Rand des Ruins, weil ihr die Banken plötzlich keinen Kredit mehr gaben. Grund: Ein versehentlicher Eintrag in die Schuldnerliste (vgl. Tz. 4.4.4). Ein Polizeibeamter, gegen den vor Jahren einmal ermittelt worden war und der sich an einer anderen Dienststelle eine „neue Existenz" aufgebaut hatte, mußte erleben, wie ihn die Schatten der Vergangenheit auch dort einholten. Grund: Seine Fingerabdrucke waren auch 9 Jahre nach dem Freispruch noch gespeichert (vgl. Tz. 4.2.1). Ein Bürger mußte 2 000 DM Verfahrenskosten bezahlen, weil weder die Behörde noch das Verwaltungsgericht erkannten, daß er ein Recht auf Akteneinsicht hat (vgl. Tz. 4.6.4). Einmal mehr zeigen diese Beispiele, daß es von vornherein „harmlose" Daten und „leichte Fehler" bei ihrer Verarbeitung nicht gibt. Es kommt vielmehr auf den Verwen-

dungszusammenhang an, wie es das Bundesverfassungsgericht im Volkszählungsurteil bereits festgestellt hat.

Die Verfahrensweisen der **Behörden** zeigen allzu häufig ein **widersprüchliches Bild**. Während auf der einen Seite die Modernisierung der Verwaltung mit allem Nachdruck vorangetrieben wird, bis hin zur Vernetzung von Behörden über Zuständigkeitsgrenzen hinweg und zur Einrichtung von Bürgerbüros, in denen „alles aus einer Hand" bearbeitet werden soll, begegnete uns andererseits das bekannte Beharrungsvermögen. Verweigerung der Akteneinsicht ohne sachlichen Grund, sondern „aus Prinzip" (vgl. Tz. 4.6.4); Beibehaltung überkommener Formulare und „bewährter" Verfahrensweisen mit der kaum verhohlenen Begründung: „Das haben wir immer so gemacht" (vgl. Tz. 4.1.3); während die Polizei mit modernster Datenverarbeitungstechnik ausgerüstet wird (vgl. Tz. 4.2.8), sind die seit Jahren verwendeten Vordrucke für Vernehmungen zu kritisieren, weil sie nicht korrekt über das Aussageverweigerungsrecht aufklären (vgl. Tz. 4.2.2); obwohl die Polizei ihre Datenverarbeitungssysteme selbständig betreibt und die Staatsanwaltschaft hierauf keinen Zugriff hat, soll ausgerechnet bei Auskunftsersuchen von Bürgern die Sachleitungsbefugnis der Staatsanwaltschaft der Auskunftserteilung entgegenstehen (vgl. Tz. 4.2.3); während die Justiz mit großem finanziellen Aufwand ihren Geschäftsstellenbetrieb automatisiert (vgl. Tz. 5.1), entspricht die Aufbewahrung der sensiblen Akten noch immer nicht den Anforderungen (vgl. Tz. 4.4.3).

Die Behörden entdecken immer mehr den Reiz der **Privatisierung**. Insbesondere die Auftragsdatenverarbeitung kommt in Mode. Vielen Behörden ist aber nicht klar, daß sie auch dann die Verantwortung für die Verarbeitung der Daten über ihre Bürgerinnen und Bürger behalten, wenn sie private Firmen damit beauftragt haben (vgl. Tz. 4.5.1). Bei mehreren Prüfungen war den öffentlichen Stellen nicht bekannt, was ihre privaten Auftragnehmer mit den ihnen überlassenen Daten im einzelnen gemacht hatten. Viele der uns vorgelegten Verträge zur Auftragsdatenverarbeitung entsprachen nicht den Vorschriften (vgl. Tzn. 4.5.1 u. 6.7.4).

Sorge bereitet die Art und Weise, mit der vielerorts geradezu hektisch die **Automatisierung der Datenverarbeitung** betrieben wird. Erfreulicherweise werden wir zwar immer häufiger mit umfangreichen Projektbeschreibungen, Konzepten und Pilotverfahren mit der Bitte um Beratung „eingedeckt". Aber trotz wortreicher Bemühungen lassen diese in der Regel nicht klar erkennen, was aus unserer Sicht das Entscheidende wäre: **Zielrichtung und Konzeption** der neuen Verfahren. Wenn aber jenseits von Leerformeln wie „Modernisierung", „Vereinfachung", „Beschleunigung", „Kosteneinsparung" usw. nicht klar definiert wird, welche konkrete Vorstellung die Verwaltung eigentlich mit einem Automationsvorhaben verbindet, ist es nicht möglich, die Konzepte an diesen Zielvorgaben zu messen. In diesen Fällen können auch wir in unseren Stellungnahmen nur „Steine statt Brot" geben: Eine präzise datenschutz-

rechtliche Beurteilung ist nur möglich, wenn die Verwaltung auch präzise Absichtserklärungen abgibt.

Gleichwohl werden landauf, landab **Millionenbeträge in neue Hard- und Software investiert**. Der kurzfristige Erfolg, aber auch das Prestige, sind nicht selten wichtiger als solide Sicherungskonzepte. Da zumeist ein objektiver oder hausgemachter Zeitdruck besteht, werden Risiken für die Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung mehr oder weniger bewußt in Kauf genommen. An die Stelle solider Verfahrenskonzepte treten sogenannte Pilotprojekte nach dem Motto: „einfach mal anfangen". Wenn dann später einmal ganze Ämter mehrere Tage geschlossen werden müssen, weil die EDV ausfällt, dann ist die überhastete Automatisierung längst auf dem Erfolgskonto verbucht.

Dabei bietet die Datenverarbeitungstechnik für die meisten Sicherheits- und Ordnungsmäßigkeitsprobleme heute selbst Lösungen an. Die **Datenschutzverordnung** des Landes gibt zudem einen brauchbaren und verläßlichen Verfahrensrahmen, um neue Projekte solide zu konzipieren und sicher umzusetzen (vgl. Tz. 6.1). Vielen ist das zu aufwendig und zu umständlich. Es muß alles schnell gehen und möglichst billig sein. Würde die Industrie nach dem gleichen Motto handeln, dann würden ihre hochkomplizierten computergesteuerten Fertigungsstraßen, Prozeßsteuerungsanlagen und Kommunikationsnetze kaum so reibungslos funktionieren. Wir meinen, daß die korrekte Abwicklung von Verwaltungsverfahren, insbesondere die Beachtung der Grundrechte der Bürgerinnen und Bürger, zumindest den gleichen Sicherheitsstandard verdienen, wie es für industrielle Anlagen und andere Abläufe in der Wirtschaft selbstverständlich ist. Selbst einem Laien auf dem Gebiet der Informatik müßte einleuchten, daß vernetzte Arbeitsplätze mit einer einheitlich aufgebauten, aber auf den Benutzer zugeschnittenen differenzierten Bedienoberfläche und eine strikte Trennung zwischen Administration und Benutzung von Systemen sicherer sind als ein Ameisenhaufen unterschiedlicher PC, in denen jeder Bearbeiter „sich selbst verwirklicht".

Die **Modernisierung der Verwaltung** ist ein vorrangiges Ziel der Landesregierung. Gegen eine Effektivierung der Arbeit der Behörden, gegen den Abbau von Bürokratie und Leerlauf, gegen die Automatisierung von Verfahren gibt es nichts einzuwenden. Im Gegenteil: Der Datenschutzbeauftragte erwartet von einer modernen Verwaltung auch den Verzicht auf Datenfriedhöfe und das Argument „das haben wir immer so gemacht" und eine möglichst weitgehende Transparenz der Datenverarbeitung gegenüber dem Bürger.

Wer allerdings die Modernisierungsdebatte ausschließlich unter dem Gesichtspunkt der Kosteneinsparung führt, gerät leicht auf ein gefährliches Gleis. Ein ganz entscheidender **Kostenfaktor** ist nämlich der **Rechtsstaat** selbst. Verfahrensrechtliche Prinzipien wie das rechtliche Gehör, die Akteneinsicht, die Rechtsmittelbelehrung, um nur wenige zu

nennen, verkomplizieren die Verfahrensabläufe. Sie sind aber in der Verfassung garantiert.

In ähnlicher Weise sehen sich datenschutzrechtliche Prinzipien der Hinterfragung ausgesetzt: Warum umständliche Sicherheits- und Ordnungsprozeduren, die Zeit und Geld kosten? Warum sich damit aufhalten, den Bürger bei der Datenerhebung über die beabsichtigte Verarbeitung aufzuklären, wo doch das erklärte Ziel die Beschleunigung der Verfahren ist. Ist nicht die Zweckbindung der Daten geradezu „Gift" für eine effektive, schlanke Verwaltung, die einmal erhobene Daten möglichst „ökonomisch" nutzen möchte? Wäre es letztendlich nicht das beste, jeder Bürger bekäme ein **einheitliches Personenkennzeichen**, unter dem alle über ihn gespeicherten Daten zusammengefaßt und genutzt werden könnten? Wieviel Leerlauf, Doppelarbeit, Leistungsmißbrauch, Steuerhinterziehung usw. könnte man auf diese Weise vermeiden?

So ließe sich vielleicht ein makellos effektiver Verwaltungsapparat erreichen. Er hätte aber mit dem Staat des Grundgesetzes nur noch wenig gemein. An die Stelle eines offenen, auf Kooperation angelegten Verhältnisses zwischen Staat und Bürgern würden letztere sich aus Furcht vor dem allwissenden Staat abkapseln und der Verwaltung mit Mißtrauen und Argwohn begegnen. Der durch und durch effektive Staat hätte das Vertrauen seiner Bürger verloren. Es ist deshalb notwendig, daß die Modernisierungsdebatte nicht einseitig auf die Kostenfrage reduziert wird, sondern daß auch der modernisierte Staat noch seine Qualität als demokratischer Rechtsstaat behält.

Mehr und mehr entwickelt sich das **Gesundheitswesen** zu einem Brennpunkt des Datenschutzes. Das jahrhundertealte Patientengeheimnis sieht sich mit geradezu revolutionären technischen Entwicklungen konfrontiert. Die Computer sind dabei, die Welt der Medizin in einer Weise zu verändern, die noch vor wenigen Jahren unvorstellbar war (vgl. Tz. 4.8.4). Dabei geht es auf dem „Medizinmarkt" um harte Interessen. Immerhin werden in Deutschland auf diesem Sektor pro Jahr ca. 450 Milliarden DM ausgegeben. Trotz dieser enormen Summe beherrscht das Thema „Sparen" die Diskussion. Gewiß ist es ein wichtiges Anliegen, zu teure oder überflüssige Behandlungsmethoden herauszufinden. Dies darf aber nicht einseitig zu Lasten der Privatsphäre der Patienten gehen. Viele wollen den „**gläsernen Patienten**", um gleichsam durch ihn hindurch Ärzte, Zahnärzte oder Krankenhäuser besser kontrollieren zu können. Uns ist es deshalb ein besonders Anliegen, daß das Patientengeheimnis nicht ständig ausgehöhlt, sondern statt dessen revitalisiert und gestärkt wird. Dabei macht man die Erfahrung, daß viele den Datenschutz besonders dann goutieren, wenn er mit den eigenen Interessen übereinstimmt. Wenden wir uns gegen neue Abrechnungs- und Kontrollverfahren der Kassen gegenüber den Ärzten, weil sie das Patientengeheimnis gefährden, erhalten wir Beifall aus der Ärzteschaft (vgl. Tz. 4.8.2). Wenden wir uns mit genau der gleichen Argumentation gegen die Forschung mit nicht

anonymisierten Patientendaten ohne Einwilligung der Betroffenen, reichen die Reaktionen von dem Vorwurf, wir gefährdeten Wissenschaft und Forschung, bis hin zum „Aussitzen" des Problems (vgl. Tz. 6.7.2).

1.1.3 Beratung

Zu einem entscheidenden Faktor unserer Arbeit hat sich die Beratung entwickelt. Es ist durchaus positiv zu werten, daß uns immer mehr Behörden mit **Beratungsersuchen** geradezu überschütten. Die Skala reicht von umfangreichen, mehrbändigen Verfahrenskonzeptionen (vgl. Tz. 6.2) über die Sitzungsvorlage für die Ratsversammlung am gleichen Tag („Könnten wir die Antwort per Fax noch heute erhalten?") bis hin zum Griff zum Telefon. Manche Mitarbeiter verbringen inzwischen einen großen Teil ihrer Dienstzeit mit telefonischen Beratungen.

Wir begrüßen diese Entwicklung, weil sie zeigt, daß der gute Wille bei vielen Stellen durchaus vorhanden ist. Es ist allemal besser, Fehler bei der Verarbeitung personenbezogener Daten von vornherein zu vermeiden, statt sie hinterher zu kritisieren. Viele Behörden haben auch entdeckt, daß wir außer effektivem Grundrechtsschutz nichts verkaufen wollen. Man weiß objektiven Rat bei der Vielfalt der Angebote auf dem Computermarkt zu schätzen. Es kommt immer häufiger vor, daß sich an einen Kontrollbesuch Beratungsgespräche von doppelter Länge anschließen. Dies kostet Zeit, bringt aber für den Datenschutz der Bürgerinnen und Bürger zählbare Vorteile.

Beträchtlichen Anteil an dieser Entwicklung hat die DATENSCHUTZ-AKADEMIE (vgl. Tz. 11.). Sie hat sich drei Jahre nach ihrer Gründung als Fortbildungseinrichtung etabliert. Die Kurse sind gut besucht, obwohl wir ihre Zahl Jahr für Jahr kontinuierlich gesteigert haben. Auch dies ist als ein Zeichen zu werten, daß es am guten Willen nicht mangelt, die datenschutzrechtlichen Vorschriften zu beachten. In diesem Bericht findet sich eine Kurzfassung des Jahresprogramms der DATENSCHUTZ-AKADEMIE. Im Text werden mit diesem Zeichen

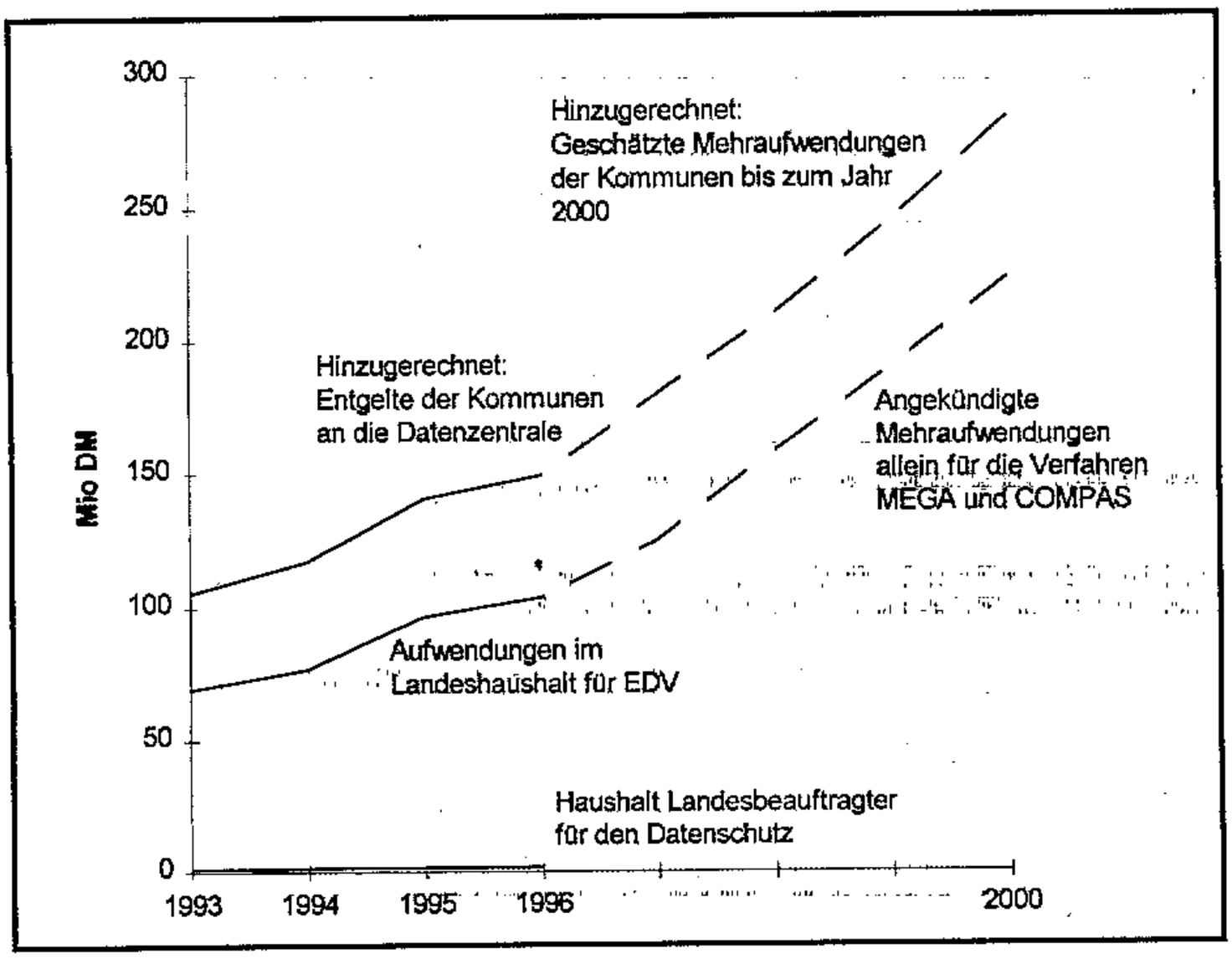


Hinweise auf thematisch einschlägige Veranstaltungen gegeben. Daraus wird ersichtlich, daß für uns Kontrolle, Beratung und Fortbildung eine Einheit bilden.

1.2 Die Ausstattung der Dienststelle

Die Dienststelle besteht jetzt aus 18 Mitarbeiterinnen und Mitarbeitern, Vorzimmerkraft, Schreibdienst, Registratur inclusive. Blickt man auf die letzten Jahre zurück, so ist festzustellen, daß seit 1993 der Personalbestand statistisch gesehen um 50 % zugenommen hat. Dies ist eine positive Entwicklung, die unterstreicht, wie sehr das Parlament in den vergangenen Jahren die Notwendigkeit einer effektiven Datenschutzkontrolle gesehen hat. In Zeiten, in denen tagaus, tagein von Sparen, Verschlankung und Personalabbau die Rede ist, ist dies alles andere als selbstverständlich. Schleswig-Holstein kann mit dieser Personalausstattung einen guten Mittelplatz unter den deutschen Datenschutzbehörden halten.

Diese erfreulichen Feststellungen erscheinen allerdings in einem anderen Licht, wenn man die zu bewältigenden Aufgaben etwas näher unter die Lupe nimmt. Dann zeigt sich nämlich, daß die elektronische Datenverarbeitung im gleichen Zeitraum um ein Vielfaches angewachsen ist.



Diese Grafik bedarf natürlich der Interpretation:

- Für das gleiche Geld bekommt man 1996 etwa doppelt soviel Computerleistung wie 1993. Die Informationstechnik wird ständig besser, aber auch schwerer zu kontrollieren. Als die Amerikaner ihre Apollo-13-Kapsel zum Mond schickten, hatten sie etwa die Rechnerleistung von zwei einfachen PC an Bord. Damit würde sich heutzutage eine Kommune mit 5 000 Einwohnern nicht mehr begnügen.

- Innerhalb der Gesamtsumme der Aufwendungen für EDV im Landeshaushalt vollziehen sich seit Jahren beträchtliche Verschiebungen. Der Anteil der Entgelte an die Datenzentrale sinkt kontinuierlich. Dies bedeutet: die Landesbehörden setzen mehr und mehr eigene Verfahren ein, was zu Technik- und Verfahrensvielfalt und damit zu einer Erschwerung der Kontrollaufgabe führt.

- Die Grafik enthält nicht das gesamte Kontrollfeld, da z.B. die Kammern und Hochschulen nicht mitgerechnet sind.

- Die Zahlen für den kommunalen Sektor sind nicht exakt zu ermitteln. Wir sind bei unserer Schätzung vorsichtig gewesen, so daß die Summen tatsächlich eher höher liegen dürften.

- In den kommenden Jahren werden sich die Zahlen für die Aufwendungen auf dem EDV-Sektor dramatisch nach oben entwickeln. Im Landesbereich steht eine Bugwelle riesiger Investitionen im EDV-Bereich bevor (vgl. Tz. 6.2). Auch in den Kommunen ist für die Jahre 97-99 ein außergewöhnlicher Investitionsschub zu erwarten, da die derzeit bei den meisten Kommunalverwaltungen betriebenen Systeme veraltet sind und vor dem Jahr 2000 abgelöst werden sollen.

Alles in allem ist die Entwicklung der Automatisierung also sogar wesentlich beeindruckender, als es die Statistik ausdrücken kann. In jedem Falle verdeutlicht sie aber, daß sich die Schere zwischen den realen Kontrollmöglichkeiten des Landesbeauftragten für den Datenschutz und der Ausstattung der Behörden mit immer mehr Computern ständig weiter öffnet. Der Zeitpunkt ist absehbar, zu dem wir allenfalls noch eine Feigenblattfunktion erfüllen können.

Bei dieser Sachlage muß die Politik eine Richtungsentscheidung treffen: Entweder sie läßt die Entwicklung treiben und nimmt in Kauf, daß sich die elektronische Datenverarbeitung bei den staatlichen Stellen immer stärker unkontrolliert entwickelt. Oder sie möchte gewährleisten, daß die Grundrechte der Bürgerinnen und Bürger auch im Informationszeitalter effektiv geschützt werden. Dann allerdings muß eine Verbindung zwischen der Anschaffung von immer mehr Computern und der Ausstattung der Kontrollinstanz gesehen werden. Dies bedeutet, daß von vornherein ein Prozentsatz der Ausgaben für neue Computer für deren Kontrolle einkalkuliert werden muß. Dies bedeutet auch, daß ein Teil des Personals, das durch Computereinsatz in den Verwaltungen eingespart wird, bei der Datenschutzkontrolle zusätzlich eingesetzt werden muß. Kurzum: Die Dynamik der Haushaltsansätze für die Datenschutzkontrolle muß mit der Dynamik der Haushaltsansätze für Computersysteme Schritt halten. Wer überall in den Verwaltungen Personal einspart und durch Computer ersetzt, ohne daß die Möglichkeiten der Datenschutzkontrolle in angemessener Weise verbessert werden, gefährdet das Recht auf informationelle Selbstbestimmung. Es führt kein Weg an weiteren

Verstärkungen der Datenschutzkontrolle vorbei, wenn man nicht bewußt das Risiko in Kauf nehmen möchte, daß das Grundrecht auf Datenschutz der Bürgerinnen und Bürger mehr und mehr ins Hintertreffen gerät.

2. Der Weg in die Computergesellschaft

2.1 Grundrechtsfreundliche Technik

Betrachtet man die Entwicklung der Datenschutzdiskussion in Deutschland in den vergangenen Jahren, so fällt auf, daß sie in starkem Maße juristisch geprägt war. Zu Recht wurde großer Wert darauf gelegt, daß personenbezogene Daten nur auf einer präzisen Rechtsgrundlage verarbeitet werden. In den letzten Jahren ist deswegen eine ganze Reihe von bereichsspezifischen Gesetzen in Kraft getreten. Das **Datenschutzrecht** ist dadurch **komplizierter** und **unübersichtlicher** geworden, so daß es diskussionswürdig erscheint, ob in dieser Form das verfassungsrechtliche Gebot der Normenklarheit noch gewährleistet ist. Viele der neuen Gesetze verfolgen nämlich offensichtlich nicht das Ziel, die Datenverarbeitung der Verwaltung zu begrenzen, sondern den „Besitzstand" gesetzlich abzusichern. Bei näherem Zusehen entpuppen sich manche dieser bereichsspezifischen „Datenschutzgesetze" als Datenverarbeitungserlaubnisgesetze (vgl. Tz. 4.6.3). Diese Tendenz wird besonders dort auf die Spitze getrieben, wo umfangreiche, wortreich-bemühte Paragraphen mit weit formulierten Generalklauseln kombiniert und damit im Ergebnis konterkariert werden. Es zeigt sich, daß die Gesetzgebung der vergangenen Jahre für das Grundrecht auf Datenschutz nicht nur Vorteile gebracht hat. Immer wieder sind Bürger enttäuscht, wenn wir ihnen mitteilen müssen, daß Verfahrensweisen, die sie zu Recht als unangemessen betrachten, in den Gesetzen zugelassen sind.

Zugleich hat sich in den vergangenen Jahren die **Technik** völlig **verändert**. Die massenhafte Verbreitung von Personalcomputern, ihre Vernetzung und ihre Kombination mit multimedialen Angeboten stellt eine mit dem traditionellen Datenschutzrecht kaum lösbare Herausforderung dar. Es wird nicht einfach sein, eine derart virulente und breit gestreute Technik mit Rechtsnormen wirksam einzufangen. Es gilt auch zu bedenken, daß dem Datenschutz unterschwellige Technikängste nicht länger zunutze kommen, weil der spielerisch-unbefangene Umgang mit den Computern für viele Menschen, vor allem der jüngeren Generation, selbstverständlich geworden ist.

Erfreulich ist daher, daß es die Dialektik des Prozesses mit sich bringt, daß die **Technik** selbst **Instrumente** entwickelt, die der Gefährdung des Grundrechts auf Datenschutz entgegenwirken. Wirkungsvolle und gleichwohl für den Alltagsgebrauch geeignete **Verschlüsselungsverfahren** bieten die Chance auf freie, nicht kontrollierbare Kommunikation und auf

Sicherung gespeicherter Daten vor unbefugter Kenntnisnahme (vgl. Tz. 6.4). Digitale Signaturen machen es möglich, Texte gegen unbefugte Veränderungen zu schützen und sicher demjenigen zuzuordnen, von dem sie stammen. Gute Programme zum Schutz personenbezogener Daten gegen unbefugten Zugriff sind heute zu vertretbaren Preisen verfügbar. Mehr und mehr werden anspruchsvolle Protokollierungsverfahren entwickelt, die es auch dem technischen Laien ermöglichen sollen, die Aktivitäten des Systemadministrators im nachhinein zu kontrollieren.

Noch besser ist es allerdings, wenn Verarbeitungssysteme so ausgestaltet sind, daß personenbezogene Daten möglichst von vornherein gar nicht oder jedenfalls nicht zentral, sondern vor Ort beim Betroffenen selbst gespeichert werden (**Prinzip der Datenvermeidung**). Gerade zu Beginn der Einführung von Multimedia-Angeboten ist es wichtig sicherzustellen, daß möglichst wenig Daten über die Kunden und Verbraucher gespeichert werden und daß sie, wenn es wirklich unumgänglich ist, möglichst beim Kunden selbst gespeichert und so früh wie möglich wieder gelöscht werden (vgl. Tz. 7.1). Die Computerisierung der Medizin auf allen Ebenen könnte auch als Chance genutzt werden, bislang bestehende Risiken für das Patientengeheimnis zu minimieren (vgl. Tz. 4.8.4).

Nach wie vor kann man allerdings feststellen, daß hochmoderne, teure Verarbeitungsanlagen zwar über schier unendlich viele Leistungsmerkmale verfügen, das Wichtigste und Naheliegendste aus der Sicht des Grundrechtschutzes aber fehlt. So weist die **neue Telefonanlage** im Bereich des Landtages und der Landesregierung zwar ein ganzes Arsenal verblüffender Leistungsmerkmale auf. Aber die Anlage kann technisch nicht das strafbare unbefugte Abhören des nichtöffentlich gesprochenen Wortes in Form des Einschaltens des **Lautsprechers** verhindern. Statt dessen müssen die Bediensteten durch eine hergebrachte Dienstanweisung daran erinnert werden, daß das Einschalten des Lautsprechers ohne Einwilligung des Gesprächspartners strafbar sein kann.

Selbstverständlich bietet die Anlage auch die Bequemlichkeit des **Direktrufs**, so daß man bestimmte Anschlüsse per Knopfdruck unmittelbar erreichen kann. Leider ist damit aber - angeblich unabänderlich - die Nebenfolge verbunden, daß die Teilnehmer am Direktruf, auch wenn sie gar nicht telefonieren wollen, sehen, wer gerade telefoniert. Da dies bei einer von Exekutive und Legislative, Regierung wie Opposition, gemeinsam genutzten Telefonanlage zu brisanten Überwachungseffekten hätte führen können, mußte der Anwendungsbereich dieses Leistungsmerkmales Schritt für Schritt eingeengt werden. Der Direktruf ist jetzt nur noch innerhalb der Ressorts zulässig und auch nur dann, wenn die Betroffenen eingewilligt haben. Dies bringt umständliche Prozeduren mit sich, die obendrein den Schönheitsfehler haben, daß sich ein Mitarbeiter wohl kaum dem Wunsch seines Vorgesetzten nach Einrichtung eines Direktrufs entziehen kann. So können sich Überwachungseffekte ergeben, die vor dem Hintergrund des allseits favorisierten kooperativen

Führungsstils durchaus kritisch hinterfragt werden können. Und das alles nur, weil sich das unerwünschte Aufleuchten eines roten Lämpchens offenbar technisch nicht verhindern läßt (vgl. Tz. 7.4).

Der Datenschutz steht in den nächsten Jahren vor der Aufgabe, **das technische Potential für das Grundrecht auf Datenschutz nutzbar zu machen**. Dazu bedarf es der richtigen Schwerpunktsetzung für die eigene Arbeit sowie der nachhaltigen Überzeugungsarbeit gegenüber den Herstellern und der Verwaltung. Die Hersteller müssen davon überzeugt werden, daß die **Kunden künftig** höhere **Qualitätsansprüche** stellen werden. Die Verwaltung muß dazu bewegt werden, grundrechtsfreundliche Technik bevorzugt einzusetzen (vgl. Tz. 4.2.5). Die Datenschutzbeauftragten selbst sollten sich verstärkt diesem Fragenkreis widmen. Die diesjährige **Sommerakademie** hat sich zum Ziel gesetzt, mit Herstellern, Wissenschaftlern, Verbraucherschützern, Politikern und Datenschutzbeauftragten über diese Fragen zu diskutieren (vgl. Tz. 12.). In den Dienststellen der Datenschutzbeauftragten wird sich in den kommenden Jahren eine Verschiebung hin zu mehr technischem Sachverstand ergeben. Zudem stellt sich die Frage, ob nicht die Datenschutzbeauftragten wegen ihrer Unabhängigkeit und des Vertrauens, das sie bei den Bürgern genießen, die idealen Stellen wären, bei denen Trustcenter und andere Vertrauensfunktionen eingerichtet werden könnten.

2.2 Der Große Lauschangriff - was kommt als nächstes?

In der Öffentlichkeit wird vielfach der Eindruck erweckt, als seien mit dem F.D.P.-Mitgliederentscheid die Würfel für die Einführung des Großen Lauschangriffs gefallen. Dabei steht die eigentliche parlamentarische Debatte erst noch bevor. Ob die für die fällige **Grundgesetzänderung** notwendige 2/3-Mehrheit im Deutschen Bundestag zu erreichen ist, wird sich erst danach zeigen. Noch bleibt die Hoffnung, daß uns das Grundgesetz auch künftig vor Abhörwanzen und geheimen Videokameras in unseren Privatwohnungen schützt.

Bei den parlamentarischen Beratungen wird sicher auch die Art und Weise eine Rolle spielen, wie in den vergangenen Monaten die **Notwendigkeit** der Einführung des Großen Lauschangriffs **relativiert** wurde. Statt der leidenschaftlichen Plädoyers in der Anfangsphase der Diskussion, daß der Große Lauschangriff unbedingt erforderlich sei zur Abwehr schwerer Gefahren für das Gemeinwohl, sind zunehmend leisere Töne zu vernehmen. Seit geraumer Zeit halten sich diejenigen bedeckt, die mit drastischen Prognosen den Lauschangriff als die Waffe gegen die Rauschgiftkriminalität und andere Kapitalverbrechen bezeichnet haben. Allenthalben wird auch in Polizeikreisen abgewiegelt. Wichtig sei der Große Lauschangriff schon, aber ein Allheilmittel sei er nun auch wieder nicht. Es gäbe schon Situationen, in denen er nützlich sein könnte. Er sei aber nur ein Mittel unter vielen, das man der Polizei nicht vorenthalten

sollte. Andere Länder hätten ihn auch, warum sollte Deutschland darauf verzichten usw.

Es macht betroffen, wenn solche Argumentationen ausreichen sollen, eines unserer zentralen Grundrechte, nämlich die Unverletzlichkeit der Privatwohnung, in der Substanz aus den Angeln zu heben. Wenn es schon reicht, daß ein Mittel gewissermaßen das „Sortiment abrundet", auf welche grundrechtlichen Garantien kann man dann noch bauen?

Andere argumentieren auch heute noch mit der **Kriminalstatistik**. Sie ist aber nur eine **Momentaufnahme der Kriminalität**, die der Polizei bekannt geworden ist. Sie beinhaltet einerseits ein hohes Dunkelfeld, z.B. im Bereich der „Weiße-Kragen-Kriminalität", besagt andererseits nichts darüber, ob die von der Polizei registrierten Strafvorwürfe tatsächlich zutreffend waren und zu einer Verurteilung der Verdächtigen geführt haben. Will man mit der Kriminalstatistik seriös umgehen, bedarf sie der wissenschaftlichen Bearbeitung. Selbst Polizeibeamte räumen unumwunden ein, daß durchaus Spielräume bei der Gestaltung der Kriminalstatistik genutzt werden. So war zu lesen, man könne einen Sachverhalt statistisch als eine Straftat erfassen, genausogut aber zum Beispiel dort wo Personaleinsparungen bei der Polizei drohen, in ein halbes Dutzend Bagatelldelikte weiter aufgliedern. Eine einzige große Wirtschaftsstraftat mit Milliardenschäden hat z.B. die registrierte organisierte Kriminalität geradezu bedrohlich anwachsen lassen.

In jedem Jahr wiederholt sich zudem das gleiche Ritual. Die Zahlen der Kriminalstatistik werden publizistisch in zumeist dramatischer Aufmachung mehrfach „verbraten": Einmal als Vorausschätzung, dann als voraussichtlicher Trend, dann als tatsächliche Statistik, dann als Landesstatistik, dann als Statistik der Polizeigewerkschaft, später wiederum als ortsbezogene Auswertung. Jedesmal eine prächtige Gelegenheit, damit Politik zu machen.

Was uns daran stört ist, daß zumeist nach der Veröffentlichung entsprechender Zahlen die **Forderungen** nach **weiteren Grundrechtseinschränkungen** nicht lange auf sich warten lassen. Würden wir phantasielos nach jeder Statistik aus dem Bereich der organisierten Kriminalität ein weiteres Grundrecht einschränken, dann wäre absehbar, daß das Grundgesetz bald in seiner Substanz ausgehöhlt wäre. Und doch hätten wir am Ende nichts erreicht. Denn im nächsten Jahr würden nach allen bisherigen Erfahrungen die Kriminalitätszahlen erneut steigen. Wahrscheinlich hätten wir bald Pest und Cholera zugleich: hohe Kriminalitätsraten und weitgehend eingeschränkte Grundrechte.

Seit Jahren werden in Deutschland die **Befugnisse** der Polizei **ständig erweitert**. Die Strafprozeßordnung ist über Jahrzehnte nur einseitig um neue Ermittlungsbefugnisse bereichert worden. In die Ausstattung der Polizei mit modernster elektronischer Technik wurden bundesweit Hun-

derte von Millionen investiert. Auch in Schleswig-Holstein steht ein gewaltiger Investitionsschub bevor (vgl. Tz. 4.2.8). Die Zahl der Polizeibeamten ist in Deutschland in den vergangenen Jahrzehnten wesentlich stärker gestiegen als das Bevölkerungswachstum. Trotzdem müssen wir Jahr für Jahr das gleiche registrieren: steigende Kriminalstatistiken.

Gleichwohl kann man der Polizei nicht den entscheidenden Vorwurf machen: Sie ist für die Kriminalität in der Gesellschaft nicht verantwortlich. Sie ist auch nicht in der Lage, Straftaten in großem Umfang zu verhindern. Obwohl alle Landespolizeigesetze im letzten Jahrzehnt mit einem ganzen Arsenal rechtsstaatlich höchst bedenklicher Vorfeldbefugnisse zur Verhütung von Straftaten ausgestattet wurden - in einigen Ländern lassen sie sogar den Großen Lauschangriff zu, um Vergehen zu verhindern -, ist die Kriminalität unablässig weiter gestiegen.

Was wir deshalb brauchen, ist eine **objektive Analyse der Wirksamkeit der polizeilichen Instrumente**. Was Telefonüberwachung, Richtmikrophone, polizeiliche Beobachtung, Rasterfahndung, längerfristige Observation usw. an Erfolgen gebracht haben, muß unvoreingenommen untersucht werden, bevor ständig weiter in diese Richtung „investiert" wird. Dabei muß auch der Frage nachgegangen werden, welche „Kosten" auf der Grundrechtsseite entstanden sind, z.B. wie häufig Unverdächtige betroffen waren. Es hat den Anschein, als sei die Polizei im Bundesgebiet an einer solchen objektiven Analyse nicht sonderlich interessiert. Um so wichtiger ist es, daß der Innenminister des Landes seine Ankündigung wahrmacht, er werde notfalls auf Landesebene eine solche Analyse erstellen lassen (vgl. Tz. 10.1).

Wenn die Spirale von Kriminalstatistik und Grundrechtseinschränkungen nicht durchbrochen und durch einen rationalen Dialog über die Ursachen der Kriminalitätsentwicklung ersetzt wird, stellt sich in der Tat die bange Frage: **Welches Grundrecht ist als nächstes dran, wenn der Große Lauschangriff abgehakt ist?,**

3. Datenschutz im Landtag

3.1 Informationsrechte des Parlaments und Datenschutz Betroffener

Die Informationsrechte des Parlaments sind ein wichtiges Mittel zur Kontrolle der Regierung. Wo die datenschutzrechtlichen Grenzen liegen, ist nach den Umständen des Einzelfalles zu beurteilen.

3.1.1 Personenbezogene Daten in Antworten auf parlamentarische Anfragen

Wir wurden um Stellungnahme zu der Frage gebeten, ob in der Antwort auf eine **Kleine Anfrage** personenbezogene Angaben über den Teilnehmerkreis an einer Fortbildungsveranstaltung der Staatskanzlei gemacht werden könnten. Während wir bei anderer Gelegenheit gegen die Bekanntgabe von **Personalaktendaten** im Zusammenhang mit Kleinen Anfragen wegen des Personalaktengeheimnisses Bedenken erhoben und Hinweise für eine weitgehende Anonymisierung gegeben hatten (vgl. 17. TB, Tz. 3.1), galt dies für eine Aufzählung der Funktionen der Lehrgangsteilnehmer nicht. Die Aussage, daß z.B. die Ministerpräsidentin, der Chef der Staatskanzlei, eine Mitarbeiterin aus dem Vorzimmer der Ministerpräsidentin, der Leiter des Büros der Ministerpräsidentin usw. an der Veranstaltung teilgenommen haben, war unbedenklich. Die Betroffenen haben nämlich in ihrer dienstlichen Eigenschaft bzw. auf dienstliche Weisung an der Veranstaltung teilgenommen. Diese Tatsache braucht vor der Öffentlichkeit zum Schutz des Persönlichkeitsrechts der Betroffenen nicht vertraulich behandelt zu werden. Besondere Umstände, die im Einzelfall eine andere Behandlung notwendig erscheinen ließen (z.B. vereinbarte Vertraulichkeit der Sitzung), lagen hier nicht vor.

3.1.2 Aktenvorlagebegehren eines Ausschusses und der Schutz von Personaldaten

Anders als beim vorherigen Fall traten datenschutzrechtliche Probleme auf, als die Opposition einen Eingriff in die Unabhängigkeit eines Richters vermutete, weil dieser zusätzlich zu seiner richterlichen Tätigkeit an das Justizministerium zur Erledigung von Verwaltungsaufgaben abgeordnet worden war. Sie verlangte vom Justizminister die Vorlage der Akten. Dabei ging es auch um **Teile der Personalakte**, mit deren Vorlage an das Parlament der Betroffene nicht einverstanden war. Auch nach unserer Auffassung war dies ohne seine Einwilligung nur zulässig, wenn die Angelegenheit in nichtöffentlicher Sitzung beraten und die Unterlagen „vertraulich" behandelt wurden. Mit diesen Maßgaben übersandte der Justizminister die erbetenen Unterlagen.

Bevor der Ausschuß über die Verfahrensweise beschlossen hatte, konnten einzelne Ausschußmitglieder bereits Einsicht in die Akten nehmen. Kurze Zeit später wurde deren Inhalt sogar öffentlich diskutiert. Die Ausschußvorsitzende hat die Mitglieder richtigerweise auf die Notwendigkeit vertraulicher Behandlung solcher Daten hingewiesen, über deren Vertraulichkeit durch den Ausschuß noch nicht beschlossen ist. Bis dahin sind die Vorgaben zu beachten, die die Regierung bei der Vorlage der Unterlagen gemacht hat.

3.1.3 Nachprüfung der Berufung eines Hochschullehrers durch den Landtag

Ähnlich war ein Fall gelagert, in dem es um einen bereits abgeschlossenen Vorgang über die **Berufung eines Hochschullehrers** ging. Am Berufungsverfahren sind nach dem Hochschulgesetz verschiedene Institutionen (Berufungsausschuß, auswärtiger Gutachter, Fachbereichskonvent) beteiligt. Erst nach deren Votum und ggf. nach mehreren Auswahldurchgängen wird der Ministerin ein Berufungsvorschlag unterbreitet. Die Auffassungen und Werturteile in den „auswärtigen Gutachten" sind bestimmten Personen zuordenbar; die Auswahlvermerke geben den Meinungsbildungsprozeß innerhalb des Ministeriums wieder.

Die Inhalte dieser Berufungsvorgänge sind zwar als **sensible Personaldaten** anzusehen, sie sind jedoch nicht dem engen Kreis der streng persönlichen Informationen zuzuordnen, deren Weitergabe an das Parlament das Bundesverfassungsgericht im Flick-Urteil als unzumutbar ansah. Immerhin handelt es sich um eine Auswahlentscheidung für eine herausgehobene Funktion im öffentlichen Dienst und um Personen, die ihre Tätigkeit zumindest partiell in der Öffentlichkeit ausüben. Aus datenschutzrechtlichen Gründen war deshalb eine generelle Verweigerung der Akteneinsicht nicht geboten. Jedoch haben wir empfohlen, den Ausschluß öffentlicher personenbezogener Beratungen und Diskussionen sowie eine Einstufung der Unterlagen nach der Geheimschutzordnung einschließlich eines Kopierverbots zu beschließen, soweit eine Aktenvorlage ohne die Einwilligung aller Betroffenen erfolgen sollte. Überdies haben wir darauf aufmerksam gemacht, daß nach dem Landesdatenschutzgesetz Bewerberdaten zu löschen sind, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt.

3.2 Keine Verwertung von Stasi-Abhörprotokollen durch den „Schubladen-Untersuchungsausschuß“

Ein parlamentarischer Untersuchungsausschuß des Landtages darf keine Unterlagen auswerten, die dem Fernmeldegeheimnis unterliegen. Die Verwendung von Stasi-Unterlagen zum Nachteil von Stasi-Opfern ist unzulässig.

Auf Bitten des Ersten Parlamentarischen Untersuchungsausschusses der 13. Wahlperiode („**Schubladen-Untersuchungsausschuß**“) haben wir ein Gutachten zu der Frage erstellt, ob und in welchem Umfang der Ausschuß die Erkenntnisse aus der Abhörtätigkeit der Staatssicherheit (Stasi) der ehemaligen DDR verwenden durfte. Der Ausschuß hatte frühere Stasi-Mitarbeiter als Zeugen vernommen und vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR ca. 800 Blatt Abhörprotokolle erhalten. Ebenso wie der Innenminister hatten wir **grundsätzliche Bedenken** gegen eine Verwertung der Erkenntnisse.

Der Ausschuß hat es ausdrücklich als mögliche Zielrichtung seiner Nachforschungen bezeichnet, daß die **Stasi-Unterlagen zum Nachteil** der vom MfS **überwachten Personen** verwendet würden. § 5 Abs. 1 des Gesetzes über die Unterlagen des früheren Ministeriums für Staatssicherheit, eine der zentralen Bestimmungen des Gesetzes, verbietet dies jedoch ausdrücklich. Die Aufbewahrung der unter grob rechtsstaatswidrigen Bedingungen erhobenen Informationen ist ohnehin nur mit den Interessen der Opfer und der Notwendigkeit einer systematischen Aufarbeitung der Stasi-Tätigkeit zu rechtfertigen. Es hätte die Intentionen des Gesetzes in ihr Gegenteil verkehrt, wenn die Unterlagen erneut zum Nachteil der Stasi-Opfer eingesetzt worden wären.

Im Wortlaut

§ 5 Abs. 1 StUG:
Die Verwendung personenbezogener Informationen über Betroffene oder Dritte, die im Rahmen der zielgerichteten Informationserhebung oder Ausspähung des Betroffenen einschließlich heimlicher Informationserhebung gewonnen worden sind, zum Nachteil dieser Personen ist unzulässig. Dies gilt nicht in den Fällen des § 21 Abs. 1 Nr. 1 und 2, wenn Angaben des Betroffenen oder Dritten sich aufgrund der Informationen ganz oder teilweise als unzutreffend erweisen.

Das gleiche Ergebnis ist aus Artikel 10 Grundgesetz (**Post- und Fernmeldegeheimnis**) herzuleiten. Der Schutzbereich dieses Grundrechts umfaßt nicht nur den Schutz gegen den Vorgang des Abhörens und des Aufzeichnens von Telefongesprächen selbst. In erster Linie ist die **Vertraulichkeit des Inhalts** des Telefongespräches **geschützt**. Mithin ist auch die Aufbewahrung von Abhörprotokollen und ihre Auswertung ein Eingriff in dieses Grundrecht. Es ist auch gerichtlich ausdrücklich anerkannt, daß in der Verwertung der aus einer Telefonüberwachung gewonnenen Unterlagen durch einen Untersuchungsausschuß ein **neuer Ein-**

griff in das grundgesetzlich garàntierte Fernmeldegeheimnis liegt. Diese Rechtsprechung, die richterlich genehmigte Telefonabhörmaßnahmen auf der Grundlage der Strafprozeßordnung zum Gegenstand hatte, muß für - nach unserem Rechtsverständnis - illegale Abhörmaßnahmen der Staatssicherheit gegen Politiker in besonderem Maße gelten. Sie wurden nämlich durchgeführt, ohne daß der Anfangsverdacht irgendeiner Straftat vorlag, weder gegen den Politiker noch gegen die abgehörten Personen. Hinzu kommt, daß dem Parlamentarischen Untersuchungsausschuß nach der Schleswig-Holsteinischen Landesverfassung Eingriffe in das Fernmeldegeheimnis gerade nicht gestattet sind.

Daß diese Auffassung auch zu einem vernünftigen Ergebnis führt, wird auch durch folgende Kontrollüberlegung deutlich: Würde die DDR noch existieren, so wären entsprechende Abhörprotokolle - einmal angenommen, das MfS hätte sie großzügig angeboten - sicher mit Empörung zurückgewiesen worden. Mit Auflösung der DDR können sich aber grundsätzliche rechtsstaatliche Überlegungen nicht plötzlich verändert haben. Wir haben deshalb dafür plädiert, die Unterlagen ungelesen an den Bundesbeauftragten zurückzusenden und die bereits durchgeführten Vernehmungen nicht zu verwerten. Der Ausschuß folgte dieser Empfehlung zunächst nicht. Darauf bemühten einige der Betroffenen die Gerichte. Sowohl das **Amtsgericht** als auch das **Landgericht Kiel bestätigten** im wesentlichen unsere Auffassung. Der Ausschuß kam im Ergebnis nicht umhin, so zu verfahren wie von uns empfohlen. Die Erkenntnisse aus der Telefonüberwachung der Stasi wurden nicht verwertet.

Was ist zu tun?
Der Bundesgesetzgeber sollte im Stasi-Unterlagengesetz für eine Klarstellung sorgen und dabei die Rechtsprechung des Amts- und des Landgerichts Kiel berücksichtigen.

3.3 Datenschutzordnung für den Landtag

In der kommenden Legislaturperiode ist mit der Verabschiedung einer Datenschutzordnung für den Landtag zu rechnen.

In Gesprächen mit den Fraktionen und mit der Landtagsverwaltung haben wir uns dafür eingesetzt, den bislang in dem Entwurf für eine Datenschutzordnung vorgesehenen Begriff der **„parlamentarischen Aufgaben“**, für die dem Parlament zugegangene personenbezogene Daten verwendet werden sollen, stärker zu **präzisieren**. Nachdem sich dies als schwierig herausstellte, wurde versucht, spezielle Regelungen für besonders sensible Daten zu schaffen. Hier zeichneten sich tragbare Lösungen ab. Es wird Sache des neugewählten Landtages sein, über die Datenschutzordnung zu beschließen. Dies sollte zügig geschehen, damit nicht immer wieder im laufenden parlamentarischen Betrieb kurzfristig über datenschutzrechtliche Fragen entschieden werden muß, die eigentlich vorab grundsätzlich geklärt werden könnten.

4. Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Ein X für eine Unterschrift

Bei der Stadt Kiel wurden Bürger, die ihre Unterschrift unter eine Volksinitiative gesetzt hatten, in der Meldedatei mit einem X gekennzeichnet. Damit sollten Mehrfachunterschriften erkannt werden. Das Verfahren war aber unzulässig.

Ein Kieler Bürger wollte seinen Reisepaß verlängern lassen. Bei der Bearbeitung stellte die zuständige Mitarbeiterin in der **Paßdatei** einen Eintrag fest, der sie zu einer Rückfrage beim Einwohnermeldeamt veranlaßte. Auf Nachfrage erklärte man dem Betroffenen, es habe sich bei dem Dateieintrag „nur" um einen **Hinweis** auf seine **Teilnahme** an der **Volksinitiative** gegen die Getränkesteuer gehandelt. Der Bearbeitung seines Antrages stünde nun nichts mehr im Wege. Der Betroffene wollte sich weder mit der Auskunft noch mit dem Dateieintrag abfinden. Er wandte sich deshalb an uns.

Wir haben bei einer unangemeldeten Prüfung vor Ort festgestellt, daß in dem betreffenden **Melderegister** die Daten sämtlicher **Einwohner markiert** waren, die an verschiedenen Volksinitiativen teilgenommen hatten. Die Speicherung im Melderegister hatte außerdem zur Folge, daß im Personalausweis- und Paßregister ein Merkmal namens „EMA-Bemerkungen" aktiviert wurde, was Ursache für die Rückfrage der Sachbearbeiterin war. Für die Bearbeitung von Ausweisanträgen war die Kenntnis dieses Sachverhalts ohne Bedeutung.

Nach Auskunft der Stadt erfolgte die Speicherung nur um zu prüfen, ob in den Unterschriftenlisten der Volksinitiativen einzelne Teilnehmer mehrfach unterschrieben hatten. Es war allerdings nicht nachvollziehbar, weshalb auch die Daten über die Teilnehmer an bereits länger zurückliegenden Volksinitiativen noch immer im Melderegister enthalten waren. Die Prüfung der Stimmberechtigung in diesen Fällen war bereits seit längerem abgeschlossen.

Das Melderecht regelt abschließend, welche personenbezogenen Daten in das Melderegister aufgenommen werden dürfen. Die Speicherung der Teilnehmer an Volksinitiativen ist nicht vorgesehen. Sie war deshalb unzulässig. Gleiches gilt für die Aktivierung des Hinweisfeldes „EMA-Bemerkungen" im Personalausweis- und Paßregister. Gerade beim Umgang mit Daten über die Wahrnehmung demokratischer Rechte ist größte Sensibilität geboten. Deshalb gehört das **Wahlgeheimnis** zu den wichtigsten besonderen Datenschutzrechten. In ähnlicher Weise muß auch mit Informationen über die Teilnahme an Volksinitiativen umge-

gangen werden. Durch die Speicherung der Daten im Melderegister hatte eine **Vielzahl von Mitarbeitern** ständigen **Zugang** zu den Angaben über Betroffene, obwohl dies zu ihrer Aufgabenerfüllung nicht erforderlich war. Akzeptabel wäre beispielsweise die kurzfristige Erfassung der Teilnehmer an den Volksinitiativen in einer besonderen Datensammlung gewesen, auf die nur der oder die mit der Prüfung von Doppelunterschriften betrauten Mitarbeiter hätten Zugriff haben dürfen. Auf unsere Beanstandung hin sind die unzulässig gespeicherten Daten von der Stadt unverzüglich gelöscht worden.

Was ist zu tun?
Alle Kommunen sollten überprüfen, ob ihr Verfahren zur Feststellung von Doppelunterschriften bei Volksinitiativen den rechtlichen Anforderungen genügt.

4.1.2 Wenn Bürger Behördenfehler ausbaden müssen

Einwohnermeldeämter dürfen Melderegisterauskünfte nur erteilen, wenn die im Auskunftsersuchen enthaltenen Daten zur Person mit denen im Melderegister exakt übereinstimmen. Es werden immer häufiger Auskünfte erteilt, obwohl sich die zugrundeliegende Anfrage erkennbar auf eine andere Person bezieht. Solche Fehler können für die Betroffenen unangenehme Folgen haben.

Ein Bürger erhielt zu seinem Erstaunen in kurzem zeitlichen Abstand einen Kraftfahrzeugsteuerbescheid vom Finanzamt über 148 DM sowie ein Urteil des örtlichen Amtsgerichtes, in dem er zur Zahlung von 6 540 DM zuzüglich 2 099 DM Verfahrenskosten verpflichtet wurde. Beide Vorgänge betrafen in Wirklichkeit eine andere Person. Auf Nachfrage erfuhr er, daß eine **unrichtige Melderegisterauskunft** der Stadt **Ursache** für die Verwechslung war. Um eine Wiederholung zu verhindern, bat er die Meldebehörde schriftlich, Melderegisterauskünfte zu seiner Person künftig mit besonderer Sorgfalt zu bearbeiten. Statt einer Antwort erhielt er jedoch die Mahnung eines Energieversorgungsunternehmens über 746 DM, die erneut auf eine unzutreffende Melderegisterauskunft der Stadt zurückzuführen war.

Nach Überprüfung der Vorgänge haben wir gegenüber der Stadt eine **Beanstandung** ausgesprochen. In seiner Antwort hat der Bürgermeister versichert: „Ich habe meine Mitarbeiterinnen und Mitarbeiter angewiesen, die bekannten datenschutz- und melderechtlichen Bestimmungen künftig genau zu beachten und insbesondere auch ausreichende Identitätsprüfungen vor Erteilung von Melderegisterauskünften ungeachtet der Vielzahl der täglich eingehenden schriftlichen und mündlichen Auskunftsersuchen vorzunehmen."

Nur **einen Monat später** erhielt der Betroffene neun Zahlungsaufforderungen der Telekom über insgesamt 5 946 DM. Ursache war wieder eine falsche Melderegisterauskunft der Stadt, obwohl im Auskunftsersuchen der Telekom auch ein Geburtsdatum angegeben worden war, das mit dem des Betroffenen nicht übereinstimmte. Der Betroffene hatte alle Hände voll zu tun, um die unberechtigten Ansprüche abzuwehren. Mit Mühe entging er einem Versäumnisurteil des Amtsgerichts. Aufgrund unserer erneuten Beanstandung hat der Bürgermeister nun den Zugriff auf die entsprechenden Meldedaten auf die Person des Amtsleiters beschränkt.

Was ist zu tun?
Bei Melderegisterauskünften ist eine sorgfältige Identitätsprüfung unverzichtbar. Ergeben sich Zweifel an der Identität, muß die Auskunft versagt werden.

4.1.3 ... das haben wir immer so gemacht

Bei einer weiteren Kontrolle gaststättenrechtlicher Erlaubnisverfahren bestätigten sich gravierende datenschutzrechtliche Mängel. Abhilfe ist zu diesem Fall nicht in Sicht, da die Verantwortlichen offenbar nach dem Motto verfahren wollen: „Das haben wir immer so gemacht".

Nachdem wir bereits im Vorjahr bei der Prüfung **gaststättenrechtlicher Erlaubnisverfahren** datenschutzrechtliche Defizite feststellen mußten, haben wir eine weitere Prüfung, dieses Mal bei einer kreisfreien Stadt, durchgeführt. Die Ergebnisse waren erneut unbefriedigend. Folgende bereits im letzten Tätigkeitsbericht aufgezeigte Rechtsverstöße (17. TB, Tz. 4.4.1) waren **erneut zu beanstanden**:

- Mängel bei der Aufklärung Betroffener,
- die Nichtbeachtung des Vorrangs der Datenerhebung beim Betroffenen,
- nicht erforderliche Regelanfragen bei örtlichen Polizeidienststellen,
- die Anforderung eines Führungszeugnisses ohne Kenntnis der Betroffenen,
- die routinemäßige Unterrichtung der Polizei über alle erteilten Erlaubnisse,
- die undifferenzierte Aufnahme von Schriftstücken in Erlaubnisakten ohne ausreichende Klärung, Prüfung und Bewertung der zugrundeliegenden Sachverhalte.

Daneben haben wir **weitere Mängel** festgestellt:

- **Anforderung und Speicherung vollständiger Mietverträge in den Erlaubnisakten**
  Soweit Antragsteller nicht selbst Eigentümer des Betriebsgrundstücks waren, hatten sie einen **Mietvertrag für die Betriebsräume** vorzulegen. Dieser wurde in vollem Umfang zur Erlaubnisakte genommen, obwohl darin eine Vielzahl von Daten enthalten waren, die für die Erteilung der Konzession nicht benötigt wurden (z.B. die Höhe der zu zahlenden Miete). Soweit tatsächlich Zweifel an der uneingeschränkten Nutzungsberechtigung des Antragstellers für die Betriebsräume bestanden, hätte als Nachweis für das Erlaubnisverfahren eine kurze Bestätigung des Vermieters ausgereicht.

- **Anhörung des Gewerbeaufsichtsamtes**
  Im Rahmen der Beteiligung anderer Behörden wurde das Gewerbeaufsichtsamt selbst dann um Stellungnahme gebeten, wenn nach den im Antrag angegebenen betrieblichen Verhältnissen nicht mit einer Beschäftigung von Arbeitnehmern zu rechnen war. Das die Zuständigkeit des Gewerbeaufsichtsamtes nach der Gewerbeordnung auf die Prüfung des technischen und sozialen Arbeitsschutzes für Arbeitnehmer beschränkt ist, war eine Datenerhebung insoweit **nicht erforderlich**.

- **Beteiligung des Bezirksschornsteinfegermeisters**
  Vor Erteilung der beantragten Erlaubnis wurde überflüssigerweise regelmäßig der für das Betriebsgrundstück zuständige Bezirksschornsteinfegermeister gehört, obwohl die Gewährleistung des Brandschutzes **Aufgabe der unteren Bauaufsichtsbehörde** ist. Diese wird im Erlaubnisverfahren ohnehin beteiligt. In Zweifelsfällen kann sie sich der Sachkunde des Bezirksschornsteinfegermeisters bedienen.

- **Dokumentationspflicht bei der Speicherung personenbezogener Daten**
  Zur Prüfung der persönlichen Zuverlässigkeit des Antragstellers wurde eine **Ermittlungsakte der Staatsanwaltschaft** unter Angabe des genauen Aktenzeichens zur Einsicht angefordert. Hinweise auf das Ermittlungsverfahren waren weder dem Antrag des Betroffenen noch der Stellungnahme der Polizei, der örtlichen Ordnungsbehörde oder dem Bundeszentralregisterauszug zu entnehmen. Auch der zuständige Mitarbeiter konnte sich an die Herkunft dieser Informationen nicht erinnern. Woher hatte die Behörde also von dem Aktenzeichen der Staatsanwaltschaft erfahren? Das Datenschutzrecht schreibt ausdrücklich vor, daß mit der Speicherung personenbezogener Daten sicherzustellen ist, daß ihre Herkunft nachvollziehbar ist.

- **Sperrung bestrittener Sachverhalte**
  Soweit Eignungsbedenken über Erlaubnisinhaber bekannt wurden, erfolgte bei erheblichen Vorwürfen eine Anhörung der Betroffenen. Widersprachen diese dem dargestellten Sachverhalt, und ließ sich die Richtigkeit der erhobenen Vorwürfe nicht nachweisen, hätte nach geltendem Datenschutzrecht eine Sperrung der Daten erfolgen, d.h., sie hätten zumindest entsprechend gekennzeichnet werden müssen. Eine Weiterverarbeitung wäre dann nur noch in eingeschränkter Form möglich gewesen. Eine **Sperrung** personenbezogener Daten war **in keinem der** geprüften **Fälle erfolgt**, so daß jederzeit das Risiko der rechtswidrigen Nutzung der Daten bestand.

- **Übermittlung vollständiger Erlaubnisakten an andere Erlaubnisbehörden**
  Auf Anforderung war eine vollständige Erlaubnisakte an die Freie und Hansestadt Hamburg zur Einsichtnahme übersandt worden. In ihr war eine Vielzahl personenbezogener Daten enthalten, die der Empfänger zur Erfüllung seiner Aufgaben nicht benötigte. Besonders unverständlich muß für die empfangende Stelle eine in der Akte enthaltene belastende **Mitteilung** des örtlichen Polizeireviers gewesen sein, aus der aber keine Folgerungen gezogen worden waren. Statt dessen war die Erlaubnis vorbehaltlos erteilt worden. Bei einer Begrenzung der Datenübermittlung auf das Erforderliche wäre eine derart negative Einschätzung nicht mit übermittelt worden.

- **Durchführung von Widerrufsverfahren**
  Wird die persönliche Unzuverlässigkeit eines Erlaubnisinhabers festgestellt, ist die erteilte Gaststättenerlaubnis unter Anordnung der sofortigen Vollziehung zu widerrufen. Gegen solche Entscheidungen war von Betroffenen über ihre Anwälte **Widerspruch** eingelegt worden. Gleichzeitig war beim Verwaltungsgericht die Wiederherstellung der aufschiebenden Wirkung der Widersprüche beantragt worden. Über die eingelegten Widersprüche war in der Hauptsache bis zum Prüfungszeitpunkt nicht entschieden worden und sollte nach Auskunft der geprüften Stelle auch nicht mehr entschieden werden. Dies hatte aber für die Speicherung der belastenden Informationen neue Folgen. Es begannen nämlich nicht die Löschungsfristen für abgeschlossene Erlaubnisvorgänge zu laufen. Außerdem bestand eine **dauerhafte Belastung** der Betroffenen durch die Speicherung der Widerrufsentscheidungen im Gewerbezentralregister.

- **Löschung von Daten**
  Erlaubnisakten wurden nach Beendigung der Gewerbeausübung abgeschlossen und aufgrund einer Dienstanweisung länger als **30 Jahre** aufbewahrt. Eine Begründung, zu welchem Zweck die Unterlagen für einen so langen Zeitraum gespeichert werden müssen, konnte nicht gegeben werden. Nach verwaltungsgerichtlicher Rechtsprechung sind Eignungsbedenken nur für einen Zeitraum von etwa fünf Jahren für

gewerberechtliche Verfahren verwertbar. Für einen wesentlichen Teil der Unterlagen waren also die Voraussetzungen des datenschutzrechtlichen Löschungsgebots längst erfüllt.

Die geprüfte Stelle hat weder während der Prüfung noch bei späteren Kontakten die Bereitschaft erkennen lassen, ihre **rechtswidrige Verwaltungspraxis** in den dargestellten Punkten zu ändern. Dabei sind wir sicher, daß eine Erfüllung der datenschutzrechtlichen Anforderungen auch zu einer Vereinfachung des Verwaltungsverfahrens und damit zu der allseits gewünschten Verschlankung der Verwaltung beitragen könnte. Der Minister für Wirtschaft, Technik und Verkehr des Landes Schleswig-Holstein wurde deshalb gebeten, **aufsichtsbehördlich tätig** zu werden. In einer ersten Reaktion hat er zum Ausdruck gebracht, daß er unsere Beanstandungen für berechtigt hält und die Stadt angehalten, künftig datenschutzgerecht zu verfahren.

Was ist zu tun?
Die geprüfte Stadt sollte ihren Rechtsstandpunkt noch einmal überprüfen. Der Wirtschaftsminister sollte gegebenenfalls aufsichtlich tätig werden.

4.1.4 Verwaltungsvorschriften für Gewerbeanzeigen verbessert

Neue Vorschriften zum Umgang mit Gewerbeanzeigen führen zur Vereinfachung des Verfahrens und zur Einstellung datenschutzrechtlich bedenklicher Verfahrensweisen.

Die Aufnahme bereichsspezifischer Datenverarbeitungsvorschriften in die Gewerbeordnung hatte zur Folge, daß auch die Verwaltungsvorschriften zum Umgang mit Gewerbeanzeigen neu gefaßt werden mußten. Arbeitsgrundlage waren zunächst bundeseinheitliche Empfehlungen, gegen die wir erhebliche datenschutzrechtliche Bedenken geltend gemacht haben. Der Minister für Wirtschaft, Technik und Verkehr zeigte sich unseren Anregungen und Forderungen gegenüber aufgeschlossen, so daß **wesentliche Verbesserungen** des ursprünglichen Entwurfstextes erreicht werden konnten.

Zu nennen sind insbesondere

- der Wegfall von Kontrollmitteilungen an andere Gewerbebehörden bei Betriebsverlagerungen,

- die Vorgabe eines Musters für die Aufklärung Betroffener über die Weiterverarbeitung ihrer Daten nach Abgabe der Gewerbeanzeige,

- die Kürzung der Speicherfrist für Daten über abgemeldete Gewerbe-

betriebe auf ein Jahr,

- die Festlegung eines datenschutzgerechten Verfahrens zur Prüfung schutzwürdiger Belange Betroffener bei der Auskunftserteilung an private Stellen,

- das Verfahren der Anforderung von Zentralregisterauskünften über die Betroffenen bei der Anmeldung sog. Vertrauensgewerbe (z.B. Ehevermittlungen, Gebrauchtwagenhandel u.ä.).

Was ist zu tun?
Die Gewerbebehörden müssen ihre Verfahrensweise der neuen Rechtslage umgehend anpassen.

4.1.5 Sitzungsprotokolle auf Diskette?

Protokolle über Sitzungen kommunaler Selbstverwaltungsgremien dürfen deren Mitgliedern zugänglich gemacht werden, soweit dies durch Beschluß, Satzung oder Geschäftsordnung festgelegt ist. Die Zuleitung der Protokolle auf elektronischen Datenträgern ist nicht ausgeschlossen, bedingt aber technische und organisatorische Sicherungsmaßnahmen.

Alle Dienststellen und Ämter einer Stadt wurden vom Hauptamt aufgefordert, die mit Textverarbeitungsprogrammen erstellten **Protokolle von Sitzungen** der Gremien den in der Ratsversammlung vertretenen **Fraktionen** nicht nur in Papierform, sondern auch **auf Diskette** zuzusenden. Damit sollte den Fraktionen die Suche nach bestehenden Beschlüssen erleichtert werden. Wir wurden gefragt, ob die Weitergabe der Disketten ebenso wie die Versendung von Protokollen auf Papier eine Datenübermittlung darstelle und ob zwischen hauptamtlichen und ehrenamtlich Tätigen in einer Kommunalverwaltung unterschieden werden müsse.

Nach der Gemeindeordnung besteht nur die allgemeine Verpflichtung, Niederschriften zu erstellen. In Literatur und Rechtsprechung wird aus der Gemeindeordnung unmittelbar abzuleitender Rechtsanspruch auf Übergabe von Sitzungsniederschriften an die Mitglieder des betreffenden Gremiums nicht gesehen. Allerdings muß mindestens die Möglichkeit der **Einsichtnahme** gegeben werden. Die kommunale Vertretungskörperschaft kann allerdings durch Beschluß, Satzung oder in der Geschäftsordnung festlegen, daß jedem Mitglied ein Exemplar der Niederschrift zuzuleiten ist. Ist dies geschehen, kann in der bloßen Zuleitung des Protokolls kein Verstoß gegen das informationelle Selbstbestimmungsrecht derjenigen gesehen werden, deren personenbezogene Daten Gegenstand der Beratung waren. Dies gilt auch dann, wenn der Text der Niederschrift in elektronischer Form, z.B. auf einer Diskette, weitergegeben wird.

Hiervon getrennt zu betrachten ist die Frage, welche **technischen und organisatorischen Maßnahmen** getroffen werden müssen, um die Beachtung der Verschwiegenheitspflicht nach der Gemeindeordnung und die Einhaltung der Datenschutzvorschriften z.B. bei ehrenamtlichen Gemeindevertretern sicherzustellen. Die Unterschiede der Protokolle (z.B. öffentliche/nichtöffentliche Beratung, Ausschußberatung/Plenarsitzung, Vertraulichkeit der Daten, Konkretisierungsgrad der Angaben) rechtfertigen unterschiedliche Maßnahmen. Während die Protokolle öffentlicher Beratungen durchweg keines erhöhten Schutzes bedürfen, müssen bei sensibleren Informationen besondere Erläuterungen zum Grad der Vertraulichkeit mit besonderem Hinweis auf die Schweigepflicht und das informationelle Selbstbestimmungsrecht, eine Markierung der ausgegebenen Protokollexemplare (Stempelaufdrucke „**vertraulich**" und Numerierungen) oder die Aufforderung zur verschlossenen Aufbewahrung der Unterlagen eine angemessene Datensicherheit bewirken. Im Einzelfall muß sogar auf die Aushändigung der Protokolle oder jedenfalls vollständiger Exemplare der Protokolle überhaupt verzichtet werden.

Was ist zu tun?
Nimmt ein Mitglied einer Vertretungskörperschaft Protokolle mit in seinen privaten Bereich, sind sie zwar der Kontrolle der Kommune und auch unserer Kontrolle entzogen; gleichwohl muß die Pflicht zur vertraulichen Nutzung und sicheren Verwahrung der anvertrauten Daten von ihm beachtet werden.

4.1.6 Datenschutz bei Wahlen

Das Wahlgeheimnis ist als ein spezielles Datenschutzrecht besonders zu schützen. Unseren Vorschlägen zur Änderung der Wahlvorschriften ist der Innenminister im wesentlichen gefolgt.

Aufgrund der Ankündigung der Landesregierung, ein **Gesetz zur Änderung wahlrechtlicher Vorschriften** zu erlassen, haben wir dem Innenminister die Berücksichtigung datenschutzrechtlich relevanter Gesichtspunkte vorgeschlagen:

- In der Gemeinde- und Kreiswahlordnung ist auf unsere Anregung hin geregelt, daß Wahlberechtigte, deren Meldedaten mit einer melderechtlichen **Auskunftssperre** versehen sind, nicht in dem auszulegenden **Wählerverzeichnis** abgedruckt werden. Diese Regelung soll auch für die Landtagswahlen in die Landeswahlordnung übernommen werden.

- Die Erstellung von **Wahlstatistiken** mit Hilfe nach Geschlecht und Altersgruppen gekennzeichneter Wahlscheine darf das **Wahlgeheim-**

nis nicht in Frage stellen. Deshalb sollten die für die Wahlstatistik herangezogenen Wahlbezirke eine Mindestzahl an Wahlberechtigten, und zwar auch in den einzelnen statistisch zu betrachtenden Altersgruppen, umfassen. Nur so erscheint es ausgeschlossen, aus einer Kombination verschiedener Persönlichkeitsmerkmale auf das Wahlverhalten einzelner zu schließen. Der Innenminister hat dies gemeinsam mit dem Statistischen Landesamt geprüft und garantiert die Einhaltung des Wahlgeheimnisses.

- Zur Wiedergewinnung von **Wahlhelfern** wollte der Innenminister die Daten der Wahlberechtigten verwenden und daraus ausgewählte Namen und Anschriften dauerhaft von der zuständigen Stelle speichern und wiederverwenden lassen. Für derartige Wahlhelferdateien gibt es nun eine Rechtsgrundlage.

Die Erteilung von **Wahlscheinen** zur Briefwahl muß beantragt und der **Antrag begründet** werden. Mit der Begründung werden personenbezogene Informationen des Wahlberechtigten erhoben (Ortsabwesenheit, körperliche Gebrechen u.a.m.). Die vorgetragenen Gründe können jedoch kaum einmal geprüft werden. Nach unserer Auffassung könnte daher überhaupt auf eine Begründung des entsprechenden Antrages verzichtet werden. Der Innenminister hält jedoch eine Begründung im Interesse der politischen Verantwortlichkeit für unverzichtbar, um den Betroffenen die bürgerliche Ehrenpflicht, persönlich zur Wahl zu erscheinen, deutlich zu machen. Er ist unserem Vorschlag daher nicht gefolgt.

Was ist zu tun?
Der Innenminister sollte versuchen, die erreichten Verbesserungen auch bei Bundestags- und Europawahlen durchzusetzen.

4.2 Polizei

4.2.1 Der lange Schatten der Vergangenheit

Nach einem Freispruch ist die Aufbewahrung erkennungsdienstlicher Unterlagen nur unter engen Voraussetzungen zulässig. Vorhandene Speicherungen müssen spätestens anläßlich einer Sachbearbeitung auf ihre Berechtigung überprüft werden. Hieran mangelt es offenbar in der Praxis. Betroffen war in einem Fall ausgerechnet ein Polizeibeamter.

Gegen einen Polizeibeamten wurde Mitte der 80er Jahre ein Ermittlungsverfahren geführt, das mit einem **rechtskräftigen Freispruch** endete. Der Betroffene wurde an eine neue Dienststelle versetzt, wo zunächst niemandem etwas von dem Ermittlungsverfahren bekannt war. Die damals angefertigten **erkennungsdienstlichen Unterlagen** wurden

jedoch weiterhin beim Landeskriminalamt (LKA) aufbewahrt. Neun Jahre danach geriet der Betroffene an seiner neuen Dienststelle erneut unter Tatverdacht, weil seine Fingerabdrücke an in der Dienststelle gelagertem Diebesgut festgestellt worden waren und sich beim Datenabgleich im LKA prompt ein „Treffer" ergab. Er hatte jedoch ein sicheres Alibi, da er zum fraglichen Tatzeitpunkt Dienst gehabt hatte. Die Fingerabdrücke waren möglicherweise beim Umräumen von sichergestelltem Diebesgut in der Dienststelle entstanden. Allerdings war nun das alte Ermittlungsverfahren wieder in aller Munde. Die Vergangenheit hatte ihn eingeholt.

Nach diesem Vorfall wurden auf Antrag unseres Petenten die über ihn gespeicherten Daten bei der Polizei **umgehend gelöscht**, so daß wir die Angelegenheit nicht mehr in allen Einzelheiten klären konnten. Eine Aufbewahrung der Unterlagen auch noch neun Jahre nach diesem Freispruch könnte nach den gesetzlichen Vorschriften nur durch ganz außergewöhnlich gravierende Umstände gerechtfertigt gewesen sein. Zudem hatte der Innenminister bereits 1993 durch Erlaß eine Überprüfung des Kriminalaktenbestandes über Polizeibeamte angeordnet. Spätestens bei dieser Gelegenheit hätten die Unterlagen vernichtet werden müssen. Denn hätten tatsächlich schwerwiegende Umstände die weitere Aufbewahrung gerechtfertigt, so hätte die Polizei wohl kaum kurze Zeit später die Daten auf Antrag des Betroffenen ohne weiteres gelöscht. Wir haben die Datenspeicherung **beanstandet**.

Was ist zu tun?
Die Polizei muß prüfen, wie sie ihre Verfahrensweise bei der Überprüfung bestehender Speicherungen verbessern kann.

4.2.2 Belehrung über das Aussageverweigerungsrecht in Vernehmungsbögen fehlerhaft

Beschuldigte in einem Strafverfahren und Betroffene eines Ordnungswidrigkeitenverfahrens können die Aussage über ihre persönlichen - etwa wirtschaftlichen oder familiären - Verhältnisse verweigern. Das von der Polizei verwendete Formular enthält seit Jahren eine fehlerhafte Belehrung über dieses Recht.

Der Beschuldigte eines strafrechtlichen Ermittlungsverfahrens muß **Angaben zu seiner Person** - Name, Ort und Tag der Geburt, Familienstand, Beruf, Wohnadresse, Staatsangehörigkeit - machen, denn er soll die für das Verfahren notwendige Identifizierung und Erreichbarkeit seiner Person gewährleisten. Über diese Angaben hinaus hat er ein **Aussageverweigerungsrecht** nach der Strafprozeßordnung. Aus verfassungsrechtlichen Gründen darf nämlich niemand dazu gezwungen werden, durch Angaben zur Sache an seiner eigenen Überführung als

Täter einer Straftat bzw. Ordnungswidrigkeit mitzuwirken. Polizei und Staatsanwaltschaft sollen allerdings im Rahmen der Vernehmung auch die sogenannten „persönlichen Verhältnisse" des Beschuldigten ermitteln. Damit sind Informationen über die wirtschaftlichen Verhältnisse und über das persönliche und berufliche Umfeld des Beschuldigten gemeint, die Aufschluß über die Schwere der Schuld und über die Angemessenheit des Strafmaßes geben können.

Diese Daten gehören allerdings zur Kategorie der **„Angaben zur Sache"**, auf die sich das Aussageverweigerungsrecht des Beschuldigten bezieht. Der von der Polizei verwandte **Anhörungsbogen** führt die Angaben zu den „persönlichen Verhältnissen" jedoch in der Rubrik „Zur Person". Da sich die Belehrung über das Aussageverweigerungsrecht nur auf die Angaben „Zur Sache" bezieht, entsteht bei den Betroffenen der Eindruck, zu Angaben über die „persönlichen Verhältnisse" seien sie verpflichtet.

Wir halten eine Neugestaltung des Anhörungsbogens, die dem Beschuldigten den Umfang seines Aussageverweigerungsrechts korrekt und zweifelsfrei verdeutlicht, für zwingend geboten. Denn das Schweigerecht des Beschuldigten zur Sache gehört zu den verfassungsrechtlichen Grundfesten des Straf- und Ordnungswidrigkeitenverfahrens. Eine endgültige Stellungnahme des Innenministers zu unserer Forderung steht noch aus.

Was ist zu tun?
Der Innenminister sollte den Anhörungsbogen der Rechtslage anpassen.

4.2.3 Auskunft durch die Polizei bei laufenden Ermittlungsverfahren

Die Polizei muß den Betroffenen darüber Auskunft erteilen, welche Daten sie zu welchem Zweck und auf welcher Rechtsgrundlage gespeichert hat. Dies gilt grundsätzlich auch bei noch laufenden Ermittlungsverfahren.

Das im Landesdatenschutzgesetz sowie in vielen Spezialgesetzen verankerte Auskunftsrecht des einzelnen über die zu seiner Person gespeicherten Daten ist ein wichtiger Bestandteil des Rechts auf informationelle Selbstbestimmung, denn der Bürger soll sich Sicherheit darüber verschaffen können, „wer was wann über ihn weiß". Im Rahmen einer Eingabe wurde uns die Praxis der schleswig-holsteinischen Polizei bekannt, bei **laufenden Ermittlungsverfahren** Antragsteller, die ihren datenschutzrechtlichen Auskunftsanspruch geltend machen, an die Staatsanwaltschaft als „verfahrensführende Stelle" zu verweisen. Der Bürger soll in diesem Falle also nicht von der Polizei, sondern von der Staatsanwaltschaft Auskunft über die aufgrund des Ermittlungsverfahrens über ihn gespeicherten Daten erhalten.

Diese Vorgehensweise ist datenschutzrechtlich nicht haltbar. Der Betroffene, nicht nur der Beschuldigte, sondern zum Beispiel auch ein Zeuge oder Hinweisgeber, möchte erfahren, welche Daten gerade die **Polizei** über ihn gespeichert hat. Da die Staatsanwaltschaft keinen unmittelbaren Zugang zu den polizeilichen Datensammlungen hat, beispielsweise zu den Kriminalakten und der Personenerkenntnisdatei PED, kann sie insoweit keine Auskunft erteilen. Die Polizei betreibt ihre Datenverarbeitung völlig selbständig. Sie fragt die Staatsanwaltschaft weder ob sie eine Kriminalakte anlegen soll, noch in welchen der vielen Polizeidateien sie Daten speichern darf, noch ob sie die Daten an andere Polizeibehörden, insbesondere an das Bundeskriminalamt, weiterübermitteln darf. Es wäre unverständlich, wenn die staatsanwaltschaftliche Verfahrensherrschaft im Bereich der polizeilichen Datenverarbeitung ausgerechnet dann zum Tragen käme, wenn ein Bürger seine datenschutzrechtlichen Ansprüche geltend macht. Auch in strafrechtlichen Ermittlungsverfahren ist die Polizei, wenn sie selbst Daten über den Beschuldigten erhebt, **datenverarbeitende Stelle** und deshalb verpflichtet, über Auskunftsbegehren selbst zu entscheiden.

Im Wortlaut
§ 198 LVwG

(1) Der betroffenen Person ist von der datenverarbeitenden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. *die zu ihr gespeicherten Daten,*
2. *den Zweck und die Rechtsgrundlage der Speicherung sowie*
3. *die Herkunft der personenbezogenen Daten, die Empfänger von Übermittlungen und die Teilnehmer an automatisierten Abrufverfahren.*

...

Die Polizei hat allerdings das Recht, eine Auskunftserteilung zu verweigern, wenn durch sie der Zweck eines laufenden Ermittlungsverfahrens gefährdet würde. Aufgrund der **strafprozessualen Verfahrensherrschaft** der Staatsanwaltschaft dürfte es in der Regel erforderlich sein, daß die Polizei eine Entscheidung der Staatsanwaltschaft darüber einholt, ob von den gesetzlichen Auskunftsverweigerungsgründen Gebrauch gemacht werden soll. Das Datenschutzrecht steht dieser verfahrensrechtlich erforderlichen Rückkopplung mit der Staatsanwaltschaft selbstverständlich nicht im Wege. Sie bleibt jedoch ein interner Vorgang und darf nicht dazu führen, daß der Bürger „von Pontius zu Pilatus" geschickt wird.

Das **Innenministerium** sieht sich allerdings zu einer Änderung der polizeilichen Praxis außerstande, da die Polizei an eine entsprechende staatsanwaltschaftliche Weisung über das Verfahren bei Auskunftsersuchen in laufenden Ermittlungsverfahren gebunden sei. Wir haben deshalb unsere Rechtsauffassung dem Generalstaatsanwalt unterbreitet und ihn gebeten, uns eine derartige Weisung zur Kenntnis zu geben. Er hat zu unserer

Anfrage bislang noch nicht Stellung genommen.

Was ist zu tun?
Die Polizei sollte auch bei laufenden Ermittlungsverfahren ihren datenschutzrechtlichen Verpflichtungen selbst nachkommen.

4.2.4 Übermittlung von Daten durch die Polizei an den Arbeitgeber einer Zeugin

Die Polizei darf ihr anläßlich eines Ermittlungsvorganges bekanntgewordene Daten nur dann an andere Behörden als Ordnungsbehörden übermitteln, wenn dies zur Abwehr einer Gefahr erforderlich ist. Diese Begründung für eine Übermittlung muß sich auch aus den Akten ergeben.

Anläßlich der Vernehmung über einen Pkw-Aufbruch zeigte die Geschädigte, eine Mitarbeiterin des örtlichen Arbeitsamtes, nach Auffassung des vernehmenden Kriminalpolizeibeamten deutliche Verhaltensauffälligkeiten. Außerdem überreichte sie dem Polizeibeamten Unterlagen über den von ihr Beschuldigten aus dessen Arbeitsamtsakte. Daraufhin übersandte die Kriminalpolizeidienststelle ihrem **Arbeitgeber** einen mehrseitigen Vermerk über die Vernehmung, in dem die Verhaltensauffälligkeiten der Zeugin detailliert geschildert wurden. Daß die Zeugin auch Teile aus der Arbeitsamtsakte des Beschuldigten übergeben und somit das Sozialgeheimnis verletzt hatte, wurde in diesem Vermerk hingegen nicht erwähnt. Eine Kopie des Berichts übersandte die Kriminalpolizei dem zuständigen Gesundheitsamt mit dem Hinweis, ein Einschreiten von Amts wegen sei unbedingt erforderlich.

Die Übermittlung dieser Daten an den Arbeitgeber der Zeugin stellt einen gravierenden Verstoß gegen das Datenschutzrecht dar und wurde von uns **beanstandet**. Unter dem Gesichtspunkt der Gefahrenabwehr, der allein eine entsprechende Datenübermittlung hätte rechtfertigen können, wäre es nur zulässig gewesen, die Tatsache der zweckwidrigen Verwendung von Arbeitsamtsakten durch die betreffende Mitarbeiterin bekanntzugeben, um weitere Vorfälle dieser Art auszuschließen. In dem übermittelten Vermerk wurde die **Mitarbeiterin** aber wegen ihres sonstigen Verhaltens bei der Zeugenvernehmung gegenüber ihrem Arbeitgeber **bloßgestellt**, der den polizeilichen Bericht prompt in einem arbeitsgerichtlichen Verfahren gegen seine Mitarbeiterin verwendete. Die Polizei hat den von uns beanstandeten datenschutzrechtlichen Verstoß anerkannt und für die Zukunft entsprechende Verhaltensanweisungen erlassen.

Die Übermittlung des Vermerks an das zuständige Gesundheitsamt war dagegen datenschutzrechtlich zulässig, da auch aufgrund früherer Vorfälle zu besorgen war, daß sowohl für die Betroffene selbst als auch für

eine dritte Person Gefahren aus ihrem Verhalten drohten.

4.2.5 Videoüberwachung erfaßt auch korrekte Autofahrer

Die schleswig-holsteinische Polizei ermittelt Verkehrsverstöße u.a. durch Videoaufzeichnungen des fließenden Autobahnverkehrs im Bereich von Autobahnbrücken. Ohne Rechtsgrundlage werden hierbei auch gesetzestreue Autofahrer erfaßt.

Auch die schleswig-holsteinische Polizei setzt seit einigen Jahren zur Ermittlung von Verkehrsverstößen, insbesondere von Überschreitungen des Sicherheitsabstandes und der Höchstgeschwindigkeit, Videomeßverfahren ein. Dabei wird der **Autobahnverkehr** über mehrere Stunden hinweg **fortlaufend aufgezeichnet** und im nachhinein in der zuständigen Polizeidienststelle auf Verkehrsverstöße ausgewertet. Die Videobänder werden zur Beweissicherung bis zum Abschluß des letzten Verfahrens aufbewahrt. Dieser Ablauf bringt es mit sich, daß die personenbezogenen Daten einer Vielzahl von **Unbeteiligten** aufgezeichnet und gespeichert werden, anders als bei den herkömmlichen Radarmessungen, bei denen Fotos erst durch den meßtechnisch ermittelten Verstoß des Verkehrsteilnehmers ausgelöst werden.

Eine den Grundsätzen des Volkszählungsurteils entsprechende Rechtsgrundlage für die Verarbeitung der Daten Unbeteiligter gibt es nach unserer Auffassung nicht. Wir haben deshalb gegenüber dem Innenminister auf eine Änderung des Verfahrens der stationären Videoverkehrsüberwachung gedrungen, nach der sich die Aufzeichnung und Speicherung personenbezogener Daten auf Personen beschränkt, gegen die der **Anfangsverdacht einer Straftat oder Ordnungswidrigkeit** vorliegt. Die Polizei sieht sich allerdings derzeit technisch und finanziell noch nicht in der Lage, entsprechende selektive Verfahren einzusetzen.

Eine derartige, **datenschutzgerechte Technik** wird in Hessen bereits eingesetzt. Videokameras erfassen durch Laserstrahlen die Pkw, deren Kennzeichen werden jedoch erst bei einem gleichzeitig in der Kamera errechneten Verkehrsverstoß kenntlich gemacht. Wir erwarten, daß für die Entwicklung und den Einsatz solcher oder ähnlicher Techniken auch bei der schleswig-holsteinischen Polizei Mittel zur Verfügung gestellt werden. Es ist rechtlich nicht zu vertreten, daß die Polizei massenhaft die Daten von Verkehrsteilnehmern erhebt und speichert, die sich völlig korrekt verhalten haben.

Was ist zu tun?
Der Innenminister sollte so schnell wie möglich eine Videotechnik einsetzen, die gesetzestreue Autofahrer nicht erfaßt.

4.2.6 Fotos vom Beifahrer werden nicht mehr herumgezeigt

Vor der Verwendung von Frontfotoaufnahmen zur Ermittlung des Fahrers bei Verkehrsverstößen werden die Beifahrer künftig unkenntlich gemacht.

Aus technischen Gründen sind auf **Frontfotoaufnahmen**, die der Ermittlung des Fahrers eines Kfz bei Verkehrsverstößen dienen, auch etwaige **Beifahrer** im Fahrzeug **sichtbar**. Läßt sich der für den Verkehrsverstoß verantwortliche Fahrer nicht anderweitig ermitteln, so kann die Polizei unter Wahrung der Verhältnismäßigkeit solche Aufnahmen auch in der Nachbarschaft des Halters des Kfz vorzeigen, um den jeweiligen Fahrer zu identifizieren. Wer Beifahrer des Verantwortlichen war, hat Dritte hierbei nicht zu interessieren und kann durchaus zu unliebsamen Enthüllungen führen. Aufgrund einer Eingabe haben wir die Polizeidienststellen in Schleswig-Holstein, die für die Vekehrsüberwachung zuständig sind, aufgefordert, Beifahrer und sonstige dritte Personen im Kfz auf den für Ermittlungszwecke verwandten Fotos **unkenntlich** zu machen. Auf den Originalnegativen allerdings müssen diese Personen aus Beweiszwecken gespeichert bleiben. Die Polizei wird künftig entsprechend verfahren.

4.2.7 Speicherung von Daten über Opfer von Straftaten

Das von der schleswig-holsteinischen Polizei betriebene POLDOK-Informationssystem zur Aufklärung von Straftaten entspricht noch nicht den Vorschriften des Landesverwaltungsgesetzes.

Wenn die Polizei strafrechtliche Ermittlungsverfahren durchführt, speichert sie die personenbezogenen Daten in der Kriminalakte und in der Polizeilichen Erkenntnisdatei. Bei bestimmten Delikten sind überdies polizeiinterne Meldedienste zu bedienen. Sie bezwecken zum einen die Unterrichtung anderer Polizeidienststellen. Andererseits sollen aber bestimmte Tatmodalitäten gesondert gespeichert und ausgewertet werden. Dieses Meldeverfahren heißt in Schleswig-Holstein POLDOK und soll jetzt automatisiert betrieben werden. Es ist naheliegend, daß POLDOK bald in das auf den polizeilichen Arbeitsplätzen verfügbare COMPAS-System integriert werden wird.

Stichwort POLDOK
Automatisiertes polizeiliches Dokumentationssystem, mit dessen Hilfe polizeiintern über die Einleitung und weitere Bearbeitung von Ermittlungsverfahren berichtet wird. Die gespeicherten Daten werden als Ermittlungsansätze in anderen Ermittlungsverfahren sowie zur Erstellung von Lagebildern verwendet.

Der Innenminister hat nun als Grundlage für den (bereits seit einigen Jahren bestehenden) Betrieb von POLDOK einen Erlaß vorbereitet, der deutlich macht, wo die datenschutzrechtlichen Probleme des Meldedienstes liegen. Gespeichert werden sollen die genauen Tatmodalitäten einschließlich der Arbeitsweise des Täters, Spuren und andere Hinweise zur Aufklärung, aber auch die personenbezogenen **Daten** des Täters sowie des **Opfers** bzw. **Geschädigten**. Die Speicherungsdauer beträgt pauschal zwei Jahre, bei herausgehobeneren Delikten jedoch zehn Jahre, wobei die überörtliche Arbeitsweise des Täters wesentliches Kriterium für diese längere Speicherungsfrist sein soll. Sobald der Tatverdacht entfallen ist, sollen die personenbezogenen Daten gelöscht werden. Eine Prüfung der Notwendigkeit der weiteren Speicherung bezüglich einer aufgeklärten Tat ist jedoch nicht vorgesehen.

Hiergegen haben wir Einwände erhoben. Die vom Landesverwaltungsgesetz vorgesehene **Einzelfallprüfung** nach Abschluß der Ermittlungen, ob die Schwere der Tat und die Wiederholungsgefahr eine Fortdauer der Speicherung rechtfertigen, soll im Rahmen von POLDOK - anders als für die Speicherung in Kriminalakten und in der PED - **nicht durchgeführt** werden. Der Gesetzgeber hat aber entschieden, daß die Polizei Daten aus einem strafrechtlichen Ermittlungsverfahren zu Zwecken der künftigen Strafverfolgung nur dann vorhalten darf, wenn es hierfür hinreichende Gründe in der Tat sowie in der Persönlichkeit des Täters gibt. Diese Anforderungen müssen insbesondere für ein automatisiertes Verfahren gelten, das - anders als die Kriminalakten - grundsätzlich jeder mit der Strafverfolgung befaßten Dienststelle der Polizei zur Verfügung steht. Es kann nicht angehen, daß bei ein und derselben Angelegenheit nur für die Aufnahme und Löschung von Daten in Kriminalakten und das damit verbundene Informationssystem (PED) die gesetzlichen Anforderungen eingehalten werden sollen, im Rahmen des POLDOK-Meldedienstes aber nicht.

Ein weiterer schwerwiegender Kritikpunkt betrifft die **Speicherung von Opfer- bzw. Geschädigtendaten**. Soweit Vorgänge, die bereits an die Staatsanwaltschaft abgegeben sind, noch für die Zwecke der künftigen Straftatenaufklärung in POLDOK gespeichert werden, gibt es für eine Speicherung von Opfer- bzw. Geschädigtendaten **keine Rechtsgrundlage**. Daß eine Person Opfer einer Straftat war, gehört - insbesondere wenn man an schwerwiegende Delikte wie etwa Sexualtaten denkt - zu den **sensibelsten Daten** der behördlichen Informationsverarbeitung überhaupt. Eine Speicherung der Namen von Opfern in Informationssystemen mit landesweiter Abrufmöglichkeit bedeutet einen **unverhältnismäßigen Eingriff** in die informationelle Selbstbestimmung der betroffenen Personen, wenn es möglich und ausreichend ist, Ermittlungsansätze durch tatbezogene Angaben über das Opfer zu erhalten.

Die diesbezüglichen Gespräche mit dem Innenminister sind noch nicht abgeschlossen. Es konnte noch keine Einigung über die unterschiedlichen

Rechtsstandpunkte erzielt werden. Der Innenminister geht bislang davon aus, daß sich die Speicherung von Daten in POLDOK nach der Strafprozeßordnung richtet. Diese enthält nach unserer Auffassung aber keine Rechtsgrundlage für die Speicherung der Daten nach Abschluß der Ermittlungen. Regelungen hierzu enthält ausschließlich das Landesverwaltungsgesetz.

Was ist zu tun?
Der Innenminister sollte unsere Rechtsauffassung im POLDOK-Erlaß berücksichtigen.

4.2.8 Computergestütztes polizeiliches Arbeitsplatzsystem (COMPAS)

Die Landesregierung hat die flächendeckende Ausstattung der schleswig-holsteinischen Landespolizei mit COMPAS bis zum Jahre 2001 beschlossen. Zu den uns bislang bekanntgegebenen Teilen des COMPAS-Konzepts haben wir detailliert Stellung genommen. Datenschutzrechtliche und -technische Verbesserungen sind geboten.

Die Einführung des „computerunterstützten polizeilichen Arbeitsplatzsystems“ bei der schleswig-holsteinischen Polizei mit einem Projektvolumen von über 65 Millionen DM schreitet voran. Beim 4. Polizeirevier in Kiel sowie im gesamten Bereich der Polizeiinspektion Plön wird bereits im Echtbetrieb mit COMPAS gearbeitet. Wir sind im Berichtszeitraum einem Ersuchen des Innenministers um **datenschutzrechtliche Beratung** für dieses Projekt gefolgt und befinden uns derzeit noch in intensiven Erörterungen über die Behebung datenschutzrechtlicher und -technischer Schwachstellen. Nach wie vor ist die Konzeption von COMPAS in vielen auch für den Datenschutz relevanten Punkten im Fluß. Einerseits kann deshalb unsere Beurteilung des Vorhabens noch nicht abschließend sein. Andererseits erwarten wir, daß vor einer weiteren „Verfestigung“ von COMPAS in der Praxis unseren datenschutzrechtlichen und -sicherheitstechnischen Bedenken und Anregungen Rechnung getragen wird.

Stichwort COMPAS
Computerunterstütztes polizeiliches Arbeitsplatzsystem, das bei der Polizei in den nächsten Jahren eingeführt wird. Es beinhaltet Funktionen der Textverarbeitung, Unterstützung der Sachbearbeitung, des Zugriffs auf polizeiliche und Verwaltungsdateien, einer erleichterten Bürokommunikation sowie der Aktenverwaltung.

Der Einsatz von COMPAS bedeutet einen **gewaltigen Qualitätssprung** in der polizeilichen Informationsverarbeitung. Die Verfügbarkeit von personenbezogenen Daten aus der polizeilichen Arbeit wird erheblich gesteigert. Nicht nur, daß das Erstellen von Briefen und Formularen erleichtert wird, jede polizeiliche Tätigkeit und die von ihr betroffenen

Personen werden künftig nicht nur in Akten, sondern zusätzlich auch in Computern gespeichert. Künftig können von jedem Arbeitsplatz aus polizeiliche Dateien wie die Fahndungsdatei, elektronische Aktennachweise, Erkennungsdienstdateien usw., aber auch Fremddateien wie das Einwohnermelderegister und die Dateien des Zentralen Verkehrsinformationssystems ZEVIS mit ca. 40 Millionen Halterdaten sowie das Verkehrszentralregister abgefragt werden. Auch die Auffindbarkeit von Daten nach Abschluß der Sachbearbeitung wird wesentlich erleichtert. Zudem beinhaltet bereitgestellte Standard-Software neben dem Programm der Vorgangsbearbeitung und -verwaltung auf jedem Arbeitsplatz die theoretisch unbegrenzte Möglichkeit zur freitextlichen Informationsverarbeitung. Es bedarf deshalb in dem sensiblen Bereich der polizeilichen Datenverarbeitung unter diesen technischen Voraussetzungen umfassender Festlegungen, die gewährleisten, daß die Bindung der Polizei an das Recht der Datenverarbeitung soweit wie möglich bereits systemseitig vorgegeben ist.

Positive datenschutzrechtliche Ansätze von COMPAS liegen nach dem derzeitigen Planungsstand beispielsweise in der systemseitigen Steuerung der Löschung von Vorgangsbearbeitungs- bzw. Vorgangsverwaltungsdaten, in der grundsätzlichen Begrenzung der Datenbestände auf die jeweilige Polizeidienststelle, in der Möglichkeit einer Zuteilung differenzierter Benutzerrechte und in der Festlegung, Personen lediglich über ihre „Verfahrensrolle", z.B. als Verdächtiger, als Anzeigenerstatter oder als Zeuge, recherchierbar zu machen. Personenbezogene Daten mit erhöhter Zweckbindung, die aus **besonderen Eingriffsmaßnahmen** wie beispielsweise der Telefonüberwachung und dem Einsatz anderer technischer Mittel gewonnen werden, sollen systemseitig besonders gesichert werden. Auch nach Abschluß der Sachbearbeitung werden in COMPAS die sogenannten Vorgangsverwaltungsdaten für eine Frist von voraussichtlich drei Jahren aufbewahrt. Damit steigert sich deren Verfügbarkeit beträchtlich. Ihre **Zweckbindung** ist kürzlich im Erlaßwege durch den Innenminister konkretisiert worden. Sie muß für die Nutzung von COMPAS auch organisatorisch umgesetzt werden.

Für folgende **Schwachstellen** von COMPAS müssen jedoch nach unserer Auffassung noch Lösungen gefunden werden:

- Neben der Speicherung von Dokumenten im computergestützten Informationssystem soll der herkömmliche, papierene Vorgang als **authentischer Datenbestand** weitergeführt werden. Aufgrund der bequemeren Verfügbarkeit von Informationen über den Bildschirm ist jedoch anzunehmen, daß bei der Sachbearbeitung weitgehend auf die automatisierte Fassung eines Vorganges zurückgegriffen werden wird. Dann muß aber gewährleistet sein, daß auch die automatisiert gespeicherten Daten vollständig und richtig sind. Wenn beispielsweise ein Zeuge seine Aussage schriftlich korrigiert, muß dies auch im Computer nachgetragen werden. Eine Festlegung, inwieweit berichti-

gende Ergänzungen aus dem Papiervorgang in die EDV zu übertragen sind, steht bislang jedoch noch aus. Kommt der Innenminister hier nicht zu konsequenten Lösungen, drohen nicht nur Verstöße gegen das Berichtigungsgebot des Landesdatenschutzgesetzes, sondern es ist nur eine Frage der Zeit, bis Polizeibeamte falsche Maßnahmen einleiten, weil sie sich auf die Aktualität der in COMPAS gespeicherten Daten verlassen haben.

- Der bisherige Einsatz von COMPAS geht nach ersten Erfahrungen mit einer ungefähren Verdreifachung der Nutzung von Daten aus polizeiexternen Verwaltungsdateien einher. Die gesteigerte Verfügbarkeit dieser Datenbestände erfordert besonderes Augenmerk auf die sachverhaltsbezogene **Protokollierung** und **Kontrolle von Abfragen.**

- Es muß noch sichergestellt werden, daß besonders sensible Daten wie beispielsweise **Personenbeschreibungen** nur zu Personen gespeichert werden, bei denen dies nach der Strafprozeßordnung und nach dem Landespolizeirecht zulässig ist. So wäre etwa die Speicherung von Aussehen, Eigenschaften und Lebensgewohnheiten von Zeugen und Hinweisgebern nur in Ausnahmefällen zulässig.



Was ist zu tun?
Der Innenminister sollte unsere Verbesserungsvorschläge berücksichtigen, bevor COMPAS in weiteren Polizeidienststellen zur Anwendung kommt.

4.2.9 EUROPOL: Jeder kann betroffen sein

Das EUROPOL-Übereinkommen ist im Juli 1995 von den EU-Mitgliedstaaten unterzeichnet worden. Der Ratifizierung stehen allerdings noch gewichtige Rechts- und Datenschutzprobleme entgegen.

Das geplante Europäische Polizeiamt soll auf Grundlage der inzwischen unterzeichneten EUROPOL-Konvention eine rechtlich problematische Stellung erhalten: Trotz seiner weitreichenden Befugnisse zur Informationsverarbeitung und -übermittlung an die Mitglied- und auch an Drittstaaten bzw. internationale Organisationen ist es unmittelbar weder einer **exekutiven** noch einer **demokratisch-parlamentarischen Kontrolle** auf europäischer oder nationaler Ebene unterstellt. Zur

Stichwort EUROPOL
Ein in Den Haag entstehendes europäisches Polizeiamt, das in erster Linie die nationalen Polizeibehörden unterstützen soll. Zu diesem Zweck sollen bei EUROPOL umfangreiche Datensammlungen aufgebaut werden. Da die EUROPOL-Konvention noch nicht ratifiziert ist, arbeitet in Den Haag derzeit noch die European Drugs Unit (EDU), die ebenfalls primär dem Datenaustausch dient.

Verhütung und Bekämpfung der internationalen Kriminalität soll EUROPOL zunächst in bezug auf den illegalen Drogen- und Nuklearhandel, die Schleuserkriminalität und den Menschenhandel, die Kraftfahrzeugkriminalität sowie spätestens nach zwei Jahren auch in bezug auf den internationalen Terrorismus tätig werden. Eine Erweiterung dieses Aufgabenbereiches auf weitere Deliktsgruppen kann durch den Rat der Europäischen Union beschlossen werden. Gleichfalls in den Zuständigkeitsbereich von EUROPOL fallen die Geldwäsche und andere, mit den genannten Straftaten „in Zusammenhang stehende Straftaten". Es ist zu befürchten, daß insbesondere diese sogenannten Zusammenhangstaten den Aufgabenkreis von EUROPOL in der Praxis kaum mehr eingrenzbar werden lassen.

Der Kreis der Personen, über die EUROPOL Daten speichern und weiterverarbeiten darf, ist so weit und in der Auslegung dehnbar, daß **praktisch jede Person** damit rechnen muß, in einer der EUROPOL-Dateien aufzutauchen: Gespeichert werden können nicht nur Tatverdächtige und Verurteilte einer Straftat, für die EUROPOL zuständig ist, sowie potentiell Tatverdächtige, sondern auch

- **potentielle Zeugen** vergangener oder künftiger Straftaten,

- Opfer vergangener Straftaten oder, bei Vorliegen bestimmter Tatsachen, **mögliche Opfer** künftiger Straftaten,

- Kontakt- und Begleitpersonen sowie Hinweisgeber.

Dieser Personenkreis geht weit über das nach schleswig-holsteinischem Datenschutz- und Polizeirecht Zulässige hinaus.

In der EUROPOL-Konvention sind drei **Typen von Informationssammlungen** bei EUROPOL vorgesehen:

- Ein **automatisiertes Informationssystem** zum Abruf für nationale Stellen und EUROPOL, in dem Täter und Tatverdächtige sowie Verurteilte gespeichert werden,

- **Arbeitsdateien** im Rahmen bestimmter Analyseprojekte, für die EUROPOL die von den Mitgliedstaaten angelieferten Daten über Täter, Tatverdächtige, Opfer, Zeugen, Hinweisgeber etc. weiterverarbeitet. Nur EUROPOL und „betroffene Mitgliedstaaten" haben direkten Zugang zu den Arbeitsdateien,

- ein **Indexsystem** zu den Arbeits- und Analysedateien.

Die nationalen Polizeien sind zwar nach der Konvention grundsätzlich dazu verpflichtet, EUROPOL die für seine Aufgaben erforderlichen Informationen zu übermitteln. Dies setzt aber auch nach der Konvention

voraus, daß beim Datenverkehr mit EUROPOL-Dateien das jeweilige **nationale Recht** eingehalten wird. Die schleswig-holsteinische Polizei darf sich also an dem Informationsaustausch über EUROPOL nur beteiligen, soweit dies das für sie geltende Landes- und Bundesrecht zuläßt.

Dennoch soll das **„Besitzerprinzip"** im europäischen Rahmen nicht durchgehalten werden. EUROPOL soll nämlich für Daten, die aus der Analysetätigkeit von EUROPOL hervorgegangen sind, selbst die datenschutzrechtliche Verantwortung für die Rechtmäßigkeit von Erhebung, Übermittlung, Richtigkeit und Überprüfung der Speicherungsfrist übernehmen. Der ursprünglich anliefernde Mitgliedstaat hat also auf die weitere Nutzung und Übermittlung der Daten dann keinen Einfluß mehr.

Erhebliche praktische und rechtliche Probleme entstehen auch für den Betroffenen einer Datenspeicherung: Ein Auskunftssuchender kann sich zwar an die Polizei eines jeden Mitgliedstaates wenden, die seinen Antrag dann an EUROPOL weiterleitet. Das **Auskunftsverfahren** richtet sich hierbei nach nationalem Recht, wird also innerhalb der EU nicht einheitlich sein. An der Entscheidung, ob dem Antragsteller Auskunft erteilt wird, müssen alle von der gespeicherten Information betroffenen Mitgliedstaaten beteiligt werden. Wird dem Antragsteller die Auskunft verweigert, kann diese Entscheidung durch die von ihm eingeschaltete gemeinsame Datenschutzkontrollinstanz von EUROPOL nur mit einer Zweidrittelmehrheit revidiert werden. Mit diesem schwerfälligen Verfahren werden zu hohe Hürden für die Auskunftserteilung durch EUROPOL aufgestellt.

Gänzlich ungelöst blieb das Problem des **Rechtsschutzes**: Bislang sind nur ein Streitbeilegungsverfahren zwischen den Mitgliedstaaten und der individuelle Rechtsschutz vor den nationalen Gerichten in Haftungsfällen geregelt. Wegen des britischen Vetos wurde eine Entscheidung über die insbesondere von den Benelux-Staaten geforderte Zuständigkeit des Europäischen Gerichtshofes sowohl für Streitigkeiten zwischen Mitgliedstaaten als auch für Klagen einzelner Bürger gegen Speicherungen bei EUROPOL auf 1996 verschoben, wobei sich eine Annäherung der Standpunkte noch nicht abzeichnet. Ohne einen judikativen Gegenpart zu EUROPOL auf europäischer Ebene sind die in der Konvention verankerten Informationserhebungs- und Verarbeitungsbefugnisse auch unter dem Gesichtspunkt der **Gewaltenteilung** nicht zu rechtfertigen.

Mittlerweile wird bereits über den Text von Durchführungsbestimmungen verhandelt. Die bislang vorgelegten Entwürfe zeigen, daß unsere Sorge, der bei EUROPOL gespeicherte Personenkreis und Datenumfang könne unvertretbar ausufern, berechtigt ist. Diese Dateien sollen offenbar zur Erstellung eines fast **lückenlosen Bildes** über die **Persönlichkeit** und das **Lebensumfeld** der gespeicherten Personen mißbraucht werden. Gemeinsam mit anderen Datenschutzbeauftragten werden wir die Verhandlungen über diese Durchführungsbestimmungen daher weiterhin mit

besonderer Wachsamkeit begleiten.

Was ist zu tun?
Der Innenminister sollte sich bemühen, den schleswig-holsteinischen Datenschutzstandard bei den weiteren Schritten zur Realisierung von EUROPOL nicht verwässern zu lassen.

4.2.10 Verfassungsbeschwerde gegen das Verbrechensbekämpfungsgesetz

Die Möglichkeiten des Bundesnachrichtendienstes zum Abhören des internationalen Fernmeldeverkehrs sind durch das Verbrechensbekämpfungsgesetz erheblich erweitert worden. Das Bundesverfassungsgericht hat die Anwendung dieser Befugnisse zu Zwecken der Strafverfolgung vorläufig eingeschränkt.

Nach dem 1994 verabschiedeten Verbrechensbekämpfungsgesetz darf der **Bundesnachrichtendienst** (BND) den internationalen, **nicht leitungsgebundenen Fernmeldeverkehr** auch zur Bekämpfung des internationalen Terrorismus, der Kriegswaffenverbreitung, des Rauschgifthandels, der Geldwäsche und -fälschung aufzeichnen und auswerten. Die Überwachung soll mit Hilfe „**geeigneter Suchbegriffe**“ - offenbar computergestützt - durchgeführt werden. Zur Verhinderung oder Verfolgung bestimmter schwerer Straftaten hat der Bundesnachrichtendienst die so gewonnenen personenbezogenen Daten an Polizei und Staatsanwaltschaft weiterzugeben.

Hiergegen hatten wir schon im Gesetzgebungsverfahren wie auch in einer Stellungnahme gegenüber dem **Bundesverfassungsgericht** Bedenken erhoben. Das Gericht hat nun aufgrund einer Verfassungsbeschwerde in einer Entscheidung über den einstweiligen Rechtsschutz festgestellt, daß Daten aus der Fernmeldeüberwachung durch den BND nur dann zu Zwecken der Strafverfolgung weitergegeben und verwendet werden dürfen, wenn „**bestimmte Tatsachen**“ den Anfangsverdacht einer der im Verbrechensbekämpfungsgesetz genannten Straftaten begründen. Ausschlaggebend für das Gericht war die hohe Bedeutung des Grundrechtes der unbeobachteten Kommunikation für den einzelnen und das Gemeinwohl, da die Gefahr einer Gesprächsüberwachung ohne zureichende Anhaltspunkte beim Bürger zu schwerwiegenden Verhaltensanpassungen und Störungen seines Kommunikationsverhaltens füh-

Stichwort Nichtleitungsgebundener Fernmeldeverkehr
Im Regelfall werden die Verbindungen im Fernmeldeverkehr über Kupfer oder Glasfaserkabel (leitungsgebunden) hergestellt. Auf einigen Streckenabschnitten benutzt die Telekom aber auch Richtfunkübertragungen. Im internationalen Verkehr werden auch Satelliten als Schaltstationen eingesetzt. Mobiltelefone sind ebenso „nichtleitungsgebunden“.

ren. Die Hauptsacheentscheidung, die eine umfassendere verfassungsrechtliche Überprüfung des Verbrechensbekämpfungsgesetzes als im einstweiligen Rechtsschutz erlaubt, wird das Bundesverfassungsgericht voraussichtlich noch 1996 erlassen.

Aus unserer Sicht ist die **Entscheidung** des Bundesverfassungsgerichts **zu begrüßen** und zu hoffen, daß auch die endgültige Entscheidung restriktiv ausfällt. Denn durch die neuen Befugnisse könnten Telefongespräche von täglich tausenden von Bürgern abgehört und ausgewertet werden, obwohl fraglich ist, daß dabei nennenswerte Erfolge für die Bekämpfung des internationalen Verbrechens erzielt werden können: Anders als der „Normalbürger" werden gut organisierte Straftäter in diesem Bereich häufig Codewörter und Verschlüsselungen benutzen, die das mit festgelegten Suchbegriffen operierende Abhörverfahren des BND weitgehend ins Leere laufen lassen. Da der BND zur Weitergabe von Informationen aus dieser Fernmeldeüberwachung an die Strafverfolgungsbehörden verpflichtet ist, würden - entgegen dem **verfassungsrechtlichen Trennungsgebot** - geheimdienstliche Aktivitäten und polizeiliche bzw. staatsanwaltschaftliche Ermittlungsarbeit ineinanderfließen. Grundlegende Garantien der Strafprozeßordnung würden ausgehöhlt, wenn die Geheimdienste auf der Basis ihrer weit gefaßten gesetzlichen Befugnisse Strafermittlungen betreiben dürften.

4.3 Verfassungsschutz

4.3.1 Übermittlung von Daten zwischen den Verfassungsschutzbehörden

Auch zwischen Verfassungsschutzbehörden dürfen nur solche personenbezogene Informationen übermittelt werden, die für die Aufgabenerfüllung des Empfängers erforderlich sind.

Der allgemeine datenschutzrechtliche Grundsatz, daß nur die **erforderlichen Informationen** an eine andere Behörden übermittelt werden dürfen, ist im Landesverfassungsschutzgesetz ausdrücklich auch für das Verhältnis zwischen den Verfassungsschutzbehörden niedergelegt worden. Die allgemeinen Zusammenarbeitspflichten der Verfassungsschutzbehörden und deren gemeinsame Aufgabe, Gefahren für den Bestand unserer Verfassung und für die Sicherheit von Bund und Ländern abzuwehren, reichen also nicht aus, um Informationen über Aktivitäten von Personen in einem Bundesland unbesehen auch allen anderen Verfassungsbehörden mitzuteilen.

Bei einer diesbezüglichen **datenschutzrechtlichen Überprüfung** der Verfassungsschutzabteilung des Innenministeriums im letzten Jahr hatten wir jedoch festgestellt, daß die übermittelten Berichte nicht in allen Fällen auf eine Erforderlichkeit der darin enthaltenen personenbezogenen

Informationen für die Aufgabenerfüllung des Empfängers überprüft worden waren. Der Innenminister argumentierte zunächst, man wolle anderen Verfassungsschutzbehörden wegen der regelmäßig überregionalen Organisation und der Mobilität der vom Verfassungsschutz beobachteten Personen alle Informationen übermitteln, die nicht erkennbar irrelevant für deren Arbeit seien. Inzwischen konnten wir uns jedoch mit der Verfassungsschutzbehörde auf eine andersgerichtete Herangehensweise, die der gesetzlichen Regelung entspricht, einigen: Nur was erkennbar erforderlich ist, wird übermittelt. In zusammenhängenden Berichten über Personengruppen werden **Informationen**, die diesem Prüfkriterium nicht genügen, **unkenntlich gemacht** oder entfernt.

4.3.2 Prüfung beim Verfassungsschutz

Neues Verfassungsschutzgesetz zeigt Wirkung, ist aber noch nicht in allen Bereichen der Datenverarbeitung umgesetzt.

Als wir in unserem 13. Tätigkeitsbericht (Tz. 4.1.3.1) über das neue **Landesverfassungsschutzgesetz** von 1991 inhaltlich berichteten, haben wir herausgehoben, daß dieses Gesetz „Ernst mache mit dem Vorsatz, mehr Datenschutz im Verfassungsschutzbereich zu garantieren". Uns ist dabei bewußt gewesen, daß dieses Gesetz für die schleswig-holsteinische Verfassungsschutzbehörde wesentliche Änderungen auch bezüglich ihrer Datenverarbeitungspraxis zur Folge haben wird. So ist die Verarbeitung personenbezogener Informationen grundsätzlich nur noch dann zulässig, wenn diese **erforderlich** sind zur Beobachtung einer im Gesetz definierten **Bestrebung und** darüber hinaus **tatsächliche Anhaltspunkte** für den Verdacht bestehen, daß die betroffene Person an derartigen Bestrebungen oder Tätigkeiten teilnimmt oder sie sich solchen Personen angeschlossen hat.

Wir haben deshalb nunmehr bei der Verfassungsschutzbehörde eine **Prüfung** mit dem Ziel durchgeführt, in Stichproben festzustellen, ob und inwieweit das Landesverfassungsschutzgesetz in Schleswig-Holstein auch in der Praxis beachtet wird. Dabei zeigte sich, daß sie bemüht gewesen ist, ihre Datenverarbeitung umgehend den gesetzlichen Vorgaben anzupassen und deshalb **umfassende Bereinigungen** ihrer früheren Datenbestände vorgenommen hat. Darüber hinaus hat sie ihre bislang noch überwiegend auf konventionelle Weise geführte „Amtsdatei" auf eine automatisierte Datenverarbeitung umgestellt (Elektronische Amtsdatei EAD). Allerdings stellte sich auch heraus, daß die vollständige Umsetzung des „neuen" Verfassungsschutzgesetzes noch nicht in allen Bereichen der Behörde abgeschlossen ist.

Erwähnenswert ist in diesem Zusammenhang folgendes:

- In Dateien gespeicherte Informationen sind spätestens nach fünf Jahren auf ihre Erforderlichkeit hin zu überprüfen und spätestens zehn Jahre nach der zuletzt gespeicherten relevanten Information zu löschen. Bei der jetzigen Verfahrensweise kommt es jedoch systembedingt zu **Überschreitungen** der gesetzlich **festgeschriebenen Zeiträume**. Der Innenminister sieht allerdings wegen der seines Erachtens geringen Anzahl von Überschreitungsfällen im jetzigen Zeitpunkt keine Notwendigkeit für eine entsprechende Änderung.

- Bei personenbezogenen Speicherungen muß erkennbar sein, aufgrund welcher ihrer Aktivitäten sie einer bestimmten **Organisation zuzurechnen** sind, denn nur dann ist die Speicherung gerechtfertigt. Dies geschah bislang noch nicht hinreichend, soll aber künftig sichergestellt werden.

- Auch wenn aus der **Skinhead-Szene** in Schleswig-Holstein insgesamt ein beträchtliches Maß an Gewaltbereitschaft hervorgeht, dürfen einzelne Personen im Zusammenhang mit Treffen von Skinheads nur dann vom Verfassungsschutz registriert werden, wenn die gesetzlichen Kriterien vorliegen. Die **bloße Teilnahme** an einer Skinhead-Veranstaltung allein reicht hierfür ebensowenig aus wie die polizeiliche Feststellung einer gemeinsamen Anreise zu derartigen Ereignissen.

Was ist zu tun?

Die Verfassungsschutzbehörde sollte unsere Verbesserungsvorschläge in die Praxis umsetzen.

4.4 Justizverwaltung

4.4.1 GAST: Abschluß einer unendlichen Geschichte

Endlich ist vom Landtag ein Gesetz für das staatsanwaltschaftliche System zur Geschäftsstellenautomation (GAST) verabschiedet worden, das wesentliche datenschutzrechtliche Verbesserungen bringt.

Nachdem wir über Jahre hinweg eine Rechtsgrundlage für das GAST-System der Staatsanwaltschaften angemahnt hatten und der Justizminister bis zum Frühjahr 1995 daran festhielt, GAST könne auf den sogenannten „Übergangsbonus" gestützt werden, für entsprechende bereichsspezifische Regelungen sei allein der Bundesgesetzgeber gefragt, brachte ein von der **F.D.P.** dem Landtag vorgelegter **Gesetzesentwurf** zu GAST Bewegung in die Diskussion. Außerdem hatte der Verwaltungsgerichtshof Kassel im Juni 1995 in einem Verfahren über Datenspeicherungen des Bundeskriminalamtes entschieden, daß der „Übergangsbonus" abgelaufen sei. Auch der Justizminister legte daraufhin den Entwurf eines „Gesetzes über die staatsanwaltschaftlichen Verfahrensregister (StARegG)" vor, das der Landtag inzwischen verabschiedet hat. An der Vorbereitung sowohl des F.D.P.-Entwurfs als auch des Regierungsentwurfs haben wir beratend mitgewirkt und daher bereits in diesem Stadium wichtige datenschutzrechtliche Gesichtspunkte einbringen können:

Stichwort GAST
Geschäftsstellenautomation der Staatsanwaltschaften, die neben Erleichterungen der Arbeit der Geschäftsstellen der Staatsanwaltschaften vor allem ein Register aller in Schleswig-Holstein anhängigen oder schon abgeschlossenen Ermittlungsverfahren beinhaltet. Insgesamt sind ca. 720 000 Personen in GAST gespeichert, gegen die ein Ermittlungsverfahren eingeleitet worden ist.

- **Zugriffsbeschränkungen**
  Nach dem neuen Gesetz werden die bei den Staatsanwaltschaften anhängigen Verfahren bei der zuständigen Staatsanwaltschaft wie bisher grundsätzlich fünf Jahre lang automatisiert gespeichert. Der gegenseitige Zugriff der Staatsanwaltschaften auf Verfahrensdaten der jeweils anderen Staatsanwaltschaften ist jedoch, in Anlehnung an die Regelung für das bundesweite staatsanwaltschaftliche Informationssystem (SISY), **auf zwei Jahre begrenzt**. Hierin liegt ein deutlicher datenschutzrechtlicher Fortschritt. Es wäre kaum nachvollziehbar, daß auf Verfahrensdaten nach dem Willen des Bundesgesetzgebers, zum Beispiel der Staatsanwaltschaft Itzehoe, die Staatsanwaltschaft Hamburg nur innerhalb einer Zweijahresfrist, die Staatsanwaltschaft Flensburg jedoch über GAST noch fünf weitere Jahre zugreifen könnte.

- **Verkürzung der Speicherungsdauer**
  Nach Ablauf der Speicherfrist dürfen Verfahrensdaten mit einem eingeschränkten Datenprofil nur noch streng zweckgebunden zur **Vorgangsverwaltung** aufbewahrt werden. Dies bedeutet, daß jedenfalls der automatisierte Datenbestand nicht mehr zum Zwecke der Strafverfolgung genutzt werden darf. Die für die Länge der Speicherungsdauer zu Zwecken der Vorgangsverwaltung einschlägigen, bundesweiten **Aufbewahrungsbestimmungen** der Justiz, die teilweise aus dem letzten Jahrhundert stammen und infolgedessen das Recht auf informationelle Selbstbestimmung nicht berücksichtigen, sind allerdings stark überarbeitungsbedürftig. Darauf haben wir den Justizminister seit Jahren hingewiesen. In der Gesetzesbegründung führte der Justizminister nun aus, daß „Schleswig-Holstein nachhaltig Bestrebungen unterstützt, die in den Aufbewahrungsbestimmungen festgeschriebenen Fristen zu verkürzen. Notfalls wird dieses Ziel - unter Aufgabe der Bundeseinheitlichkeit - lediglich auf Landesebene verwirklicht werden." Wir werden ihn in dieser Frage, die auch die Aufbewahrung der papierenen Verfahrensakten betrifft, beim Wort nehmen. Inzwischen zeichnet sich bereits eine länderübergreifende Verkürzung der Fristen für die Aufbewahrung von Strafakten auf zehn bis fünfzehn Jahre ab.

- **Daten von Opfern und Geschädigten**
  In „Verfahren von besonderer Bedeutung" sieht das Gesetz eine **Speicherung** der **Namen** von **Opfern oder Geschädigten** vor, solange das Verfahren noch als Unbekanntsache geführt wird. Die Begründung des Justizministers hierfür lautet, daß es mit Hilfe des Namens des Opfers bzw. Geschädigten ermöglicht werden müsse, bei entsprechenden Anfragen etwa von Versicherungen schnell auf die zugehörige Verfahrensakte zugreifen und neuen Hinweisen zur Aufklärung der Tat rascher nachgehen zu können. Wir halten diese **Begründung** für die Speicherung von Opferdaten in GAST, die der F.D.P.-Entwurf im übrigen nicht vorsah, für **nicht stichhaltig**: Auch bei Ermittlungsverfahren, die bereits gegen einen bekannten Beschuldigten geführt werden, kann die Staatsanwaltschaft ja offenbar Anfragen auch ohne automatisierten Zugriff auf den Namen des Opfers beantworten, da sie mit der Angabe von Aktenzeichen, Tatort und -zeit etc. genügend Zuordnungsmöglichkeiten zu einem konkreten Verfahren hat. Es stimmt auch nicht, daß Opfer bzw. Geschädigte gerade bei schwerwiegenderen Straftaten damit einverstanden sind, in einem automatisierten System gespeichert zu sein. Allerdings ist nicht zu verkennen, daß das Gesetz die Gefahr einer mißbräuchlichen Nutzung von Opferdaten reduziert: Es erlaubt den **Zugriff** auf diese Daten nur dem **zuständigen Staatsanwalt**. Opferdaten sind also weder landesweit noch innerhalb einer Staatsanwaltschaft durch alle Dezernenten abrufbar. Im übrigen hat sich der Justizminister darauf festgelegt, den Katalog der „Verfahren von besonderer Bedeutung" einer kritischen Überprüfung zu unterziehen.

- **Datenverschlüsselung**
  Das Gesetz sieht ferner einen wirksamen Schutz der in GAST gespeicherten Daten gegen den unbefugten Zugriff Dritter bei der Übermittlung vor. In dem Maße, wie Verfahren zur **Verschlüsselung** von Datenbeständen „Stand der Technik" und wirtschaftlich realisierbar werden, verstehen wir unter einem „wirksamen Schutz" auch diese Form des Datenschutzes durch Technik.



4.4.2 „Ähnlichenservice" zu Lasten Unbeteiligter

Ist die Schreibweise des Namens eines Beschuldigten nicht genau bekannt, so werden aus dem bundeseinheitlichen staatsanwaltschaftlichen Informationssystem (SISY) alle Erkenntnisse über Personen mitgeteilt, deren Namen eine ähnliche Schreibweise aufweisen. Der Empfänger hat die nicht relevanten Daten unverzüglich zu löschen.

Nachdem der Bundestag bereits die Rechtsgrundlagen für die Errichtung eines staatsanwaltschaftlichen Informationssystems auf Bundesebene geschaffen hatte, sind nunmehr die detaillierten Ausprägungen des Systems in Form einer Errichtungsanordnung festgelegt worden. Trotz heftiger Proteste der Datenschutzbeauftragten des Bundes und der Länder hat man einen sogenannten „**Ähnlichenservice**" vorgesehen. Ist die Schreibweise des Namens eines Beschuldigten nicht genau bekannt, so werden die gespeicherten Erkenntnisse über Personen mit Namen ähnlicher Schreibweise ebenfalls übermittelt. Dies begegnet datenschutzrechtlichen Bedenken, weil dadurch in erheblichem Umfang personenbezogene Informationen von Menschen übermittelt werden, die mit dem konkret anhängigen Ermittlungsverfahren, für das die Abfrage durchgeführt worden ist, nichts zu tun haben.

Stichwort SISY
Ein beim Generalbundesanwalt geplantes Informationssystem, in dem bundesweit alle eingeleiteten strafrechtlichen Ermittlungsverfahren zwei Jahre lang gespeichert werden sollen.

Wir haben aber immerhin erreicht, daß diese Daten dann nicht auch noch in der Akte verbleiben, bis deren Aufbewahrungsfrist abgelaufen ist. In der Errichtungsanordnung wurde vielmehr festgelegt, daß nach erfolgter Identifizierung eines Beschuldigten die ähnlichen, jedoch andere Personen betreffenden Daten zu vernichten sind. War eine Identifizierung nicht möglich, sind alle übermittelten Daten zu vernichten.

Was ist zu tun?
Die Staatsanwaltschaften sollten nicht erforderliche Daten, die sie im Rahmen des „Ähnlichenservice" aus SISY erhalten, umgehend löschen.

4.4.3 Verfahrensakten bei der Justiz nicht immer in besten Händen

In Prozeßakten enthaltene personenbezogene Daten sind häufig äußerst sensibel und müssen deshalb besonders gegen den Zugriff unbefugter Dritter geschützt werden.

Prozeßakten enthalten häufig auch äußerst intime Informationen. Sei es, daß in Strafverfahren das persönliche Umfeld Verdächtiger penibel ausgeleuchtet, in Familiensachen „schmutzige Wäsche" gewaschen wird oder in Zivil- oder Verwaltungsgerichtsstreitigkeiten medizinische Gutachten eingeholt werden. Sie geben in vielfältiger Weise Auskunft über **persönliche Lebensverhältnisse** von Menschen. Ihre Aufbewahrung wird jedoch der Sensibilität der darin enthaltenen Informationen nicht immer gerecht. Will man Presseberichten Glauben schenken, so stellt es keine Schwierigkeit dar, Verfahrensakten aus den Dienstgebäuden der Justiz zu entwenden.

Auf unsere Nachfrage beim Justizminister, wie Prozeßakten bei der Justiz aufbewahrt würden, wurde uns mitgeteilt, diese würden zwar „so gut wie immer" in **verschließbaren Räumen**, dort jedoch in der Regel in **offenen Hängeregistratursystemen** aufbewahrt.

Zwar haben unsere Bemühungen dazu geführt, daß Akten nicht mehr wie früher in offenen Regalen auf den Fluren zu finden sind, sondern zwischenzeitlich wenigstens in verschließbaren Räumen aufbewahrt werden. Dort sind sie jedoch nur in Ausnahmefällen (Verschlußsachen) besonders gesichert. Jeder, der zum Raum einer Geschäftsstelle Zutritt hat, kommt auch ungehindert an die Akten heran. Zwar bestehen Dienstanweisungen, die Räumlichkeiten auch beim kurzfristigen Verlassen zu verschließen. Diese Dienstanweisungen werden aber offenbar nicht durchgängig befolgt. Darüber hinaus haben das Reinigungspersonal und andere externe Dienstleister außerhalb der Geschäftszeiten mangels Aufsicht ungehinderten Zugriff auf die Akten, in der Regel stehen bei der Reinigung eines Flures sogar sämtliche Räume offen. Dieser Zustand kann auf Dauer nicht hingenommen werden. Justizakten müssen ihrem sensiblen Inhalt entsprechend in **verschlossenen Behältnissen** oder in besonders gesicherten Diensträumen gelagert werden (vgl. hierzu auch Tzn. 4.5.1 und 4.10.1).



Kurz vor Fertigstellung des Berichts teilte der Justizminister ergänzend mit, er werde „im Rahmen der zur Verfügung stehenden Haushaltsmittel bestrebt sein, den Anteil verschließbarer Registraturschränke ... zu erhöhen". Außerdem werde er „dafür Sorge tragen, daß während der täglichen Reinigungsarbeiten jeweils nur die unmittelbar zu reinigenden Büroräume geöffnet werden. Damit soll vermieden werden, daß während der Reinigungsarbeiten ganze Zimmerfluchten offen stehen."

Was ist zu tun?
Der Justizminister sollte die Datensicherheit zügig bei allen Gerichten entsprechend unseren Vorschlägen verbessern.

4.4.4 Kleine Nachlässigkeiten mit großen Wirkungen

Nachlässigkeiten bei der Führung des Schuldnerverzeichnisses können für die Betroffenen verheerende Folgen haben. Die Gerichte haben deshalb bei Eintragungen und Auskünften höchste Sorgfalt zu beachten.

Eine Petentin benötigte zur Erweiterung ihres Geschäftsbetriebes ein Darlehen. An welche Bank sie sich jedoch auch wandte, niemand war bereit, ihr das Geld zu leihen. Nach vielen ausweichenden Begründungen erhielt sie schließlich von einem privaten Geldverleiher den tatsächlichen Grund für diese ungewöhnliche Zurückhaltung genannt: Eine Handelsauskunftei habe ihm mitgeteilt, sie habe im Jahre 1992 die eidesstattliche Versicherung abgegeben. Auch nachdem die Petentin den Nachweis erbracht hatte, daß die Schulden längst bezahlt und die Eintragungen in der **Schuldnerliste** des Vollstrekkungsgerichtes gelöscht waren, fand sich die private Auskunftei nicht bereit, die offensichtlich falschen Daten zu löschen. Sie berief sich auf eine telefonische Auskunft eines Amtsgerichts, das mitgeteilt habe, die Petentin sei dort immer noch im Schuldnerverzeichnis registriert.

Stichwort Schuldnerverzeichnis
Ein bei den Amtsgerichten geführtes Register der Personen, die die eidesstattliche Versicherung abgegeben haben oder gegen die im Zusammenhang damit Haft angeordnet ist. Die Eintragung bleibt in der Regel drei Jahre gespeichert. Prinzipiell kann jeder Auskunft aus dem Schuldnerregister erhalten. Industrie- und Handelskammern, Betreiber privater regionaler oder bundesweiter Auskunfteien können Abdrucke des gesamten Schuldnerverzeichnisses erhalten.

Auch unsere Nachforschungen bestätigten dies. Die Petentin war tatsächlich von einem Amtsgericht zur Abgabe der eidesstattlichen Versicherung aufgefordert worden. Dieses hatte den Vorgang jedoch an das für den Wohnort der Petentin zuständige Gericht übersandt, damit dort **in Amtshilfe** die eidesstattliche Versicherung entgegengenommen werden konnte. **Versehentlich** trug das nur in Amtshilfe tätige Amtsgericht den Vorfall dann in die dort geführte **Schuldnerliste** ein. Obwohl beim Vollstreckungsgericht die Eintragung in der Schuldnerliste nach Begleichung der Schuld gelöscht wurde, blieb die Eintragung bei dem lediglich in Amtshilfe tätig gewordenen Gericht erhalten. Erst nach Aufforderung durch uns wurde die Angelegenheit bereinigt.

Diesen Vorfall haben wir zum Anlaß genommen, den Justizminister aufzufordern, auf eine sorgfältige Bearbeitung dieser Vorgänge bei allen Amtsgerichten im Lande Schleswig-Holstein hinzuwirken. Die Gerichte haben durch entsprechende **organisatorische Vorkehrungen** und erhöhte Aufmerksamkeit sicherzustellen, daß in einem so belastenden Bereich wie dem Schuldnerverzeichnis derart schwerwiegende Fehler in Zukunft ausgeschlossen werden.

Was ist zu tun?

Die Gerichte müssen beim Umgang mit dem Schulderverzeichnis so sorgfältig wie möglich verfahren.

4.4.5 Ist Post vom Gerichtsvollzieher stets „Verschlußsache"?

Steckt der Gerichtsvollzieher Benachrichtigungen in den Hausbriefkasten, so müssen sie in der Regel in einem Briefumschlag verschlossen sein.

Gerichtsvollzieher, die Schulnder nicht in der Wohnung angetroffen haben, hinterlassen eine **Benachrichtigung**, in der auf die Folgen künftiger ergebnisloser Vollstreckungsversuche hingewiesen wird. Ein Petent hatte ein solches Schriftstück in seinem Briefkasten als **offene Karte** vorgefunden. Seine daraufhin erhobene Beschwerde begründete er damit, daß sowohl seine minderjährigen Kinder als auch die für ihn tätige Raumpflegerin den Briefkasten leerten und somit von dem gegen ihn laufenden Zwangsvollstreckungsverfahren Kenntnis hätten erlangen können. Er vertrat die Ansicht, derartige Schriftstücke müßten in jedem Falle verschlossen sein.

In der Regel weiß der Gerichtsvollzieher nicht definitiv, wer Zugriff zum Briefkasten hat. Deshalb hat er die für den Betroffenen unter Umständen peinliche Preisgabe einer laufenden Zwangsvollstreckung durch Verwendung eines **verschlossenen Briefumschlages** zu vermeiden. Der notwendige Aufwand erscheint angesichts der schutzwürdigen Belange des Empfängers denkbar gering. Der Gerichtsvollzieher muß nur außer seinen Benachrichtigungen noch einige Briefumschläge mit sich führen. Wird das Benachrichtigungsformular geringfügig umgestaltet (Querformat statt Längsformat, so daß die Adresse in einem Umschlagfenster erscheint), so braucht nicht einmal die Adresse doppelt geschrieben zu werden.

Was ist zu tun?

Die Gerichtsvollzieher sollten unseren Verbesserungsvorschlag künftig beachten.

4.5 Umweltschutz

4.5.1 Privatisierung der Abfallentsorgung

Bei der Privatisierung der Abfallentsorgung darf der Datenschutz der Bürger nicht auf der Strecke bleiben. Die Kreise behalten die datenschutzrechtliche Verantwortung auch dann, wenn sie sich privater Firmen bedienen. Diese Erkenntnis setzt sich aber erst allmählich durch.

Der Markt der **Abfallentsorgung** ist in Bewegung. Mit einer bemerkenswerten **Dynamik** verändern sich die Bedingungen und die handelnden Akteure. Obwohl die Abfallentsorgung gesetzliche Aufgabe der Kreise ist, sind in erster Linie **private Gesellschaften** am Werk. Verwundert nehmen die Bürger zur Kenntnis, daß ihnen Bescheide von einer GmbH zugehen oder daß ihre Widersprüche von einer Privatfirma „behandelt" werden. Sie sind verunsichert, und sie fragen uns, wer überhaupt in diesem Zusammenhang Daten erheben darf, wie diese Daten an private Gesellschaften gelangen und zu welchen Zwecken sie dort verwendet werden. Wir haben uns deshalb die Verfahrensweise bei einigen Kreisen etwas genauer angesehen. Dabei haben sich folgende Probleme ergeben.

- **Fehlende Rechtsgrundlagen für die Datenerhebung**

Einige Kreise haben zwar viele Aspekte der Abfallentsorgung in Satzungen bis ins Detail geregelt, nicht aber die Datenerhebung. Da auch die einschlägigen Gesetze keine entsprechenden Regelungen enthalten, ergab sich die Situation, daß eigentlich keine personenbezogenen Daten hätten erhoben und verarbeitet werden dürften und so der Abfallentsorgung das entscheidende Fundament gefehlt hätte.

Der Kreis Schleswig-Flensburg erkannte dies sogleich und nahm unsere Beratung bei der Erarbeitung entsprechender Satzungsregelungen in Anspruch. Herausgekommen sind dabei Bestimmungen, aus denen klar ersichtlich ist, welche Daten der Kreis aus welchen Quellen erheben darf und zu welchen Zwecken die Daten anschließend verwendet werden dürfen. Inzwischen gehen immer mehr Kreise dazu über, diese oder ähnliche Regelungen auch in ihren Satzungen zu treffen.

- **Dürfen die Daten an private Gesellschaften weitergeleitet werden?**

Die Kreise haben die **Abfallentsorgung** in weitem Umfang an private Gesellschaften übertragen. Auch das **Gebühreninkasso** und die dazugehörige **Datenverarbeitung** lassen sie von **privaten Firmen** erledigen. Nach dem Wortlaut des Abfallwirtschaftsgesetzes kann die

Gebührenerhebung nur auf andere öffentliche Stellen, nicht aber auf private Unternehmen übertragen werden. Private Stellen können lediglich für die Errechnung der Gebührenhöhe und den Versand von Bescheiden im Namen der zuständigen Stellen, also nur mit Hilfsfunktionen, eingeschaltet werden.

Auf unsere Nachfragen hin hat der Innenminister mitgeteilt, er lege das Kommunalabgabengesetz so aus, daß das Steuergeheimnis nur für kommunale Steuern, nicht aber für sonstige Abgaben gelte. Das Steuergeheimnis stehe folglich der Einschaltung Privater nicht entgegen. Wir haben uns nur mit Vorbehalt dieser Meinung anschließen können, denn der Wortlaut des Gesetzes läßt durchaus auch die gegenteilige Auffassung zu. Wir haben daher empfohlen, bei nächster Gelegenheit die **Rechtslage klarzustellen** und das Kommunalabgabengesetz entsprechend zu ändern. Der Innenminister hat mitgeteilt, er wolle unserer Anregung folgen.

- **Wie muß der Auftrag an die private Stelle aussehen?**

  Ist eine Privatfirma beauftragt worden, so bestimmt sich das weitere Verfahren nach den Vorschriften des Landesdatenschutzgesetzes zur **Auftragsdatenverarbeitung**. Danach behält der Auftraggeber, also die Kommune, die volle Verantwortung für die Datenverarbeitung, also auch für die Teile, die beim privaten Auftragnehmer ablaufen.

  Wir haben festgestellt, daß Datenbestände und Datenverarbeitung den privaten Entsorgern weitgehend unkontrolliert überlassen wurden. Manchen Kreisen war überhaupt nicht bekannt, was mit den Daten im einzelnen bei den Privatfirmen geschah. So staunten die Mitarbeiter des Kreises nicht weniger als unser Prüfer, als dieser bei einer Routineabfrage seine eigenen Daten gespeichert fand. Dabei wohnte er in einem ganz anderen Kreis. Weitere Nachforschungen ergaben, daß sich die Abfallentsorgungsfirma der EDV-Anlage einer weiteren Firma bediente. Dort waren die Daten aus mehreren Kreisen - der Einfachheit halber, wie gesagt wurde - zusammengeführt und in einer gemeinsamen Datenbank gespeichert worden.

  Daraus war ein unter verschiedenen Gesichtspunkten „interessanter" Datenbestand entstanden. Zum einen hatte sich zumindest in der Datenbank ein „Konzentrationsprozeß" vollzogen, den der Gesetzgeber mit der Zuweisung der Abfallentsorgung an die Kreise gerade nicht gewollt hatte. Zum anderen gehört wenig Phantasie dazu sich vorzustellen, daß je nach sonstigen Geschäftszweigen der auftragnehmenden Firma hier die unterschiedlichsten Verwendungszwecke denkbar sind. Der Bürger dürfte aber zu Recht verärgert sein, wenn seine für Zwecke der Abfallentsorgung erhobenen Daten plötzlich für irgendeine Werbung Verwendung fänden.

- Die **betroffenen Kreise wußten** nach eigenem Bekunden **nichts** von dieser Datenorganisation, ein sicheres Indiz, daß der Auftraggeber nicht mehr „Herr der Daten" war. Wir haben deshalb gegenüber den betroffenen Kreisen förmliche Beanstandungen ausgesprochen. Im Kreis Schleswig-Flensburg haben wir an einer Änderung der Verträge zwischen dem Kreis und der Abfallwirtschaftsgesellschaft sowie deren weiteren Unterauftragnehmern mitgearbeitet. Durch die **neuen Verträge** werden die Auftragnehmer z.B. verpflichtet, die Zweckbindung in allen Phasen der Datenverarbeitung einzuhalten, es werden klare Auflagen bezüglich des EDV-Einsatzes gemacht, und es werden jederzeitige Kontrollen durch den Auftraggeber und durch uns vereinbart. Inzwischen haben auch andere Kreise, nachdem wir die dortigen vertraglichen Regelungen ebenfalls beanstandet hatten - in einem Vertrag hieß es z.B. lapidar, beim Gebühreninkasso sei „der Datenschutz einzuhalten" -, ihre Verträge nachgebessert. Ob damit der Datenschutz der Bürgerinnen und Bürger in den Fällen der Einschaltung privater Firmen bei der Abfallentsorgung künftig tatsächlich gewährleistet wird, werden **weitere Kontrollen** zeigen.

- **Was nicht auf Privatfirmen übertragen werden darf**

  Eine Eingabe richtete sich dagegen, daß ein Kreis Widersprüche gegen die Abfallgebührenfestsetzung von der privaten Abfallwirtschaftsgesellschaft beantworten ließ. Dabei verfolgte er nach eigenem Bekunden das Ziel, den Bürger in Form einer Beratung davon zu überzeugen, daß die Gebührenfestsetzung rechtens sei, und damit zur Rücknahme seines Widerspruches zu veranlassen.

  Wir stellten fest, daß zwischen dem Kreis und der Abfallwirtschaftsgesellschaft überhaupt keine vertraglichen Regelungen über die Verarbeitung personenbezogener Daten bestanden. Deshalb haben wir die Weitergabe von Daten an die private Firma generell beanstandet. Überdies haben wir deutlich gemacht, daß eine Übertragung der Aufgabe, Widerspruchsbescheide zu erlassen, auf Privatfirmen nicht zulässig ist.

- **Was hat nach Beendigung der Auftragsverarbeitung mit den Daten zu geschehen?**

  Ein Kreis hatte seit Jahren zwei kreisangehörige Städte durch öffentlich-rechtlichen Vertrag mit der Aufgabe der Abfallentsorgung und damit verbunden dem Gebühreninkasso betraut. Die Wahrnehmung der Aufgabe erfolgte im Namen und im Auftrag des Kreises auf der Grundlage des Landesabfallwirtschaftsgesetzes. Bei der Datenverarbeitung handelte es sich um Datenverarbeitung im Auftrag im Sinne des Landesdatenschutzgesetzes. Da der Kreis nunmehr die Aufgaben wieder an sich gezogen hat, kann er vom bisherigen Auftragnehmer auch die dort vorhandenen personenbezogenen Daten der Betroffenen



rückübernehmen. Die betroffenen Städte waren lediglich als Auftragnehmer tätig, so daß der Kreis als Auftraggeber datenverarbeitende Stelle geblieben war. Das gleiche gilt natürlich, wenn Auftragsverhältnisse mit privaten Firmen beendet werden und diese die überlassenen Daten zurückzugeben haben.

Was ist zu tun?
Der Innenminister sollte sich für eine Präzisierung der Rechtslage im Kommunalabgabengesetz verwenden. Die Kreise sollten ihre datenschutzrechtliche Verantwortung auch bei der Privatisierung der Abfallentsorgung konsequent wahrnehmen.

4.5.2 Wann kommen die Verordnungen im Umweltrecht?

Während der Schutz personenbezogener Daten im Naturschutz durch die Datenschutzverordnung Naturschutz mittlerweile konkret geregelt ist, läßt sich das Umweltministerium mit den entsprechenden Datenschutzvorschriften nach dem Landeswassergesetz und dem Abfallwirtschaftsgesetz viel Zeit.

Die **Datenschutzverordnung Naturschutz** wurde durch das Umweltministerium **zügig erarbeitet** und in Kraft gesetzt, so daß nunmehr klare Detailregelungen das Naturschutzgesetz ergänzen.

Für den Bereich des **Abfallwirtschaftsgesetzes und des Wassergesetzes** kann eine solche **positive Bilanz nicht gezogen** werden. Auch in diesen Gesetzen sind Ermächtigungen zum Erlaß konkretisierender Datenschutzverordnungen enthalten. Trotz mehrfacher Aufforderungen, die Verordnungen „auf den Weg zu bringen", reagierte das Umweltministerium lediglich mit der Mitteilung, daß für das Landesabfallwirtschaftsgesetz **„demnächst"** mit einem ersten Entwurf für eine Datenverarbeitungsverordnung zu rechnen sei. Für eine entsprechende Vorschrift zum Landeswassergesetz könne jedoch wegen der Vielzahl der einzuschaltenden nachgeordneten Behörden frühestens Mitte 1996 mit der Aufnahme entsprechender Tätigkeiten begonnen werden.

Wie notwendig die Konkretisierung der generalklauselartigen Formulierungen in den genannten Gesetzen ist, zeigt die Problematik der Aufgabenprivatisierung im Bereich der Abfallwirtschaft (s. Tz. 4.5.1).

Was ist zu tun?
Das Umweltministerium sollte jetzt die notwendigen Verordnungen ohne weitere Verzögerung erlassen.

4.6 Wirtschaft, Technik und Verkehr

4.6.1 Schnelle Reaktion auf unsere Kontrollergebnisse

Aufgrund der letztjährigen Prüfungsergebnisse hat das Verkehrsministerium kurzfristig reagiert. Den Fahrerlaubnisbehörden sind klare Regelungen für den Datenschutz an die Hand gegeben worden.

Die im Vorjahr gewonnenen Erkenntnisse über die Datenverarbeitungspraxis der Führerscheinstellen haben das Verkehrsministerium davon überzeugt, daß einheitliche und präzise Regelungen zur automatisierten und konventionellen Datenverarbeitung bei den Fahrerlaubnisbehörden geschaffen werden müssen. Das Ministerium hat unsere Vorschläge **zügig in Verwaltungsvorschriften umgesetzt**. Ein Erlaß regelt nunmehr die Speicherfristen in Akten, die Aktenbereinigung, die Aktenführung sowie Aufbewahrungsfristen für Akten, die Speicherinhalte und Speicherfrist bei elektronischer Speicherung sowie die Datenübermittlungen an die Polizei. Ob die Führerscheinstellen die Vorschriften des Erlasses in der geforderten Weise umsetzen bzw. umgesetzt haben, gilt es durch entsprechende Nachkontrollen festzustellen.

Nicht so prompt reagierte eine Führerscheinstelle, deren Verfahrensweise wir im Jahre 1994 beanstandet hatten (vgl. 17. TB, Tz. 4.6.1). Eine **Nachkontrolle** ergab, daß noch immer keine personellen Maßnahmen ergriffen worden waren, um den fehlerhaften EDV-Datenbestand zu korrigieren und eine nicht mehr aktuelle Altkartei endlich zu vernichten. Obwohl wir dies beim Landrat ausdrücklich monierten, steht für den Abgleich der Altkartei mit dem EDV-Bestand eine personelle Verstärkung der Führerscheinstelle offensichtlich noch immer nicht in Aussicht. Nach dem Erlaß des Verkehrsministers sind die Altkarteibestände bis 31.12.1996 zu vernichten. Wir werden aufmerksam verfolgen, ob die Führerscheinstellen diese Frist einhalten.



Was ist zu tun?
Die Fahrerlaubnisbehörden sollten ihre Datenbestände nach Maßgabe der neuen Verwaltungsvorschriften umgehend bereinigen.

4.6.2 Speicherung personenbezogener Daten aufgrund der Erteilung von Taxenkonzessionen umgehend neu geregelt

Einem Taxiunternehmer hielt eine Zulassungsbehörde viele Jahre zurückliegende Verkehrsverstöße vor, weil Auskünfte aus dem Verkehrszentralregister selbst dann noch aufbewahrt wurden, als sie dort längst gelöscht waren. Das Verkehrsministerium reagierte auf unsere Kritik binnen 14 Tagen mit einem Erlaß.

Nach dem Personenbeförderungsgesetz dürfen Genehmigungen zur Personenbeförderung mit Taxen maximal für vier Jahre ausgesprochen werden. Bei Wiedererteilungen prüft die Genehmigungsbehörde, ob Eintragungen im Verkehrszentralregister vorliegen. So auch im Falle eines Petenten, der seit Mitte der 70er Jahre als Taxiunternehmer tätig ist. Er bekam seine Konzession jedesmal anstandslos verlängert. In seiner **Konzessionsakte** fanden sich jedoch einige Auszüge aus dem **Verkehrszentralregister**, die dort längst getilgt waren. Als sich nun im letzten Antragsverfahren der Bürger über den Umgangston der Behörde beschwerte, hielt diese ihm daraufhin alle von ihm begangenen Verkehrsverstöße, die sie in ihrer Akte noch gespeichert hatte, vor.

Wir haben diese Speicherungspraxis **beanstandet**. Das Personenbeförderungsgesetz legt zwar keine besonderen Speicherfristen fest. Dies bedeutet gleichwohl, daß Daten, soweit sie nicht mehr zur Aufgabenerfüllung erforderlich sind, unverzüglich zu löschen sind.



Das **Verkehrsministerium** hat sich unserer Auffassung uneingeschränkt angeschlossen und die Zulassungsbehörden aufgefordert, ihre Akten umgehend auf zu löschende Informationen durchzusehen und zu bereinigen. Bemerkenswert ist, daß die Anweisung an die Zulassungsbehörden bereits 14 Tage, nachdem dem Verkehrsministerium der Sachverhalt durch uns bekannt wurde, erging. Dies hebt sich von den langen Reaktionszeiten anderer Behörden wohltuend ab.

Was ist zu tun?
Die Zulassungsbehörden sollten die notwendige Bereinigung der Daten so zügig durchführen, wie das Verkehrsministerium auf unsere Kritik reagiert hat.

4.6.3 Bundesgesetzgeber plant weitere Verdatung der Autofahrer

Die bislang bekanntgewordenen Entwürfe zur Änderung des Straßenverkehrsgesetzes verheißen nichts Gutes. Die geplante Einführung eines zentralen Fahrerlaubnisregisters stößt auf datenschutzrechtliche Bedenken.

Mit der Änderung des Straßenverkehrsgesetzes und der Einführung der Fahrerlaubnisverordnung trägt der Bundesgesetzgeber den Vorgaben der **EG-Führerscheinrichtlinie** Rechnung, durch die das Fahrerlaubniswesen in der Europäischen Union harmonisiert werden soll. Neben den örtlichen Fahrerlaubnisregistern soll ein **neues zentrales Register** beim **Kraftfahrt-Bundesamt** eingerichtet werden, in dem alle Inhaber einer Fahrerlaubnis mit Namen, Geburtsdatum und den Fahrerlaubnisklassen registriert sind. Es soll nach Auffassung der Bundesregierung den europäischen Nachbarn ermöglichen festzustellen, ob ein deutscher Fahrer, der im europäischen Ausland aufgefallen ist, eine Fahrerlaubnis besitzt. Für die deutschen Verkehrsbehörden sowie für die Polizei soll das zentrale Fahrerlaubnisregister Vorteile bringen. Nach Meinung des Bundesverkehrsministers erfordert der Abfrageaufwand bei den derzeit über 700 örtlichen Fahrerlaubnisbehörden für Polizei, Ordnungsbehörden und europäische Dienststellen eine zentrale Datei zur Verwaltungsvereinfachung.

Wir halten diese Argumente nur zum Teil für stichhaltig und sehen das Problem, daß hier de facto ein letztlich europaweites zentrales Einwohnermelderegister eines Großteils der Bevölkerung aufgebaut wird, während bislang ein Bundesmelderegister aus guten Gründen abgelehnt wurde. Die Entwürfe des Straßenverkehrsgesetzes und der Fahrerlaubnisverordnung zeichnen sich außerdem durch **komplizierte Vorschriften** und **unübersichtliche Verweisungen** aus. Kettenverweisungen über drei oder vier Stationen sind nicht gerade das, was man unter Normenklarheit von Vorschriften versteht. Überdies regeln die Entwürfe die umfangreiche Datenverarbeitung im Bereich der Verkehrsverwaltung nur sehr lückenhaft. Wir haben unsere Kritikpunkte dem Verkehrsminister zugeleitet und gebeten, sie im Gesetzgebungsverfahren zu berücksichtigen.

Was ist zu tun?
Der Verkehrsminister sollte unsere Position im anstehenden Gesetzgebungsverfahren gegenüber dem Bund unterstützen.

4.6.4 Bürgerunfreundlich aus Prinzip?

Eine Behörde verweigerte einem Bürger die Akteneinsicht nicht aus sachlichen Gründen, sondern „aus Prinzip". Die Folge waren ein für den Bürger kostspieliger Prozeß und eine datenschutzrechtliche Beanstandung.

Ein Bürger hatte zufällig davon Kenntnis erlangt, daß in seiner Zulassungsakte Informationen gespeichert waren, die auf eine gezielte polizeiliche Überwachung seiner notärztlichen Tätigkeit, für die sein Privatfahrzeug mit Blaulicht und Einsatzhorn ausgestattet war, hindeuteten. Er begehrte daraufhin von der Zulassungsbehörde **Akteneinsicht**, ohne daß er sich auf eine konkrete Rechtsgrundlage berief. Der Kreis verweigerte ihm die Akteneinsicht unter Hinweis darauf, daß ein Anspruch nach dem Landesverwaltungsgesetz nicht gegeben sei, da in dem Verwaltungsverfahren, mit dem ihm die Sonderrechte (Blaulicht und Einsatzhorn) eingeräumt wurden, seinem Antrag voll entsprochen worden sei. Der Auskunftsanspruch nach dem Datenschutzschutzrecht wurde dabei weder vom Rechtsamt des Kreises noch von der Widerspruchsbehörde, die über den Widerspruch gegen die Ablehnung der Akteneinsicht entscheiden mußte, gesehen.

Die Angelegenheit fand schließlich vor **Gericht** ihre Fortsetzung. Das Verwaltungsgericht lehnte das Begehren des Bürgers mit denselben Gründen wie die Verwaltung ab. Auch dabei wurde der datenschutzrechtliche Auskunftsanspruch übersehen. Dem Petenten entstanden Kosten von ca. 2 000 DM. Daraufhin wandte er sich an uns.

Bei unserer Prüfung stellten wir fest, daß keinerlei Gründe gegen die Akteneinsichtnahme nach dem Landesdatenschutzgesetz vorlagen. Es zeigte sich sogar, daß die Zulassungsbehörde eigentlich nichts gegen die Akteneinsicht hatte. So heißt es in der Akte an einer Stelle: „Es gibt in der Sache zwar nichts zu verheimlichen. Es geht jedoch um die grundsätzliche Klärung, ob jede abgeschlossene Angelegenheit durch Akteneinsicht wieder aufgerollt werden muß." Die weitere handschriftliche Notiz eines Bearbeiters zeigt ein krasses Beispiel bürgerunfreundlichen Verwaltungshandelns. Dort heißt es: „Die Gewährung von Akteneinsicht wäre zwar mit weniger Aufwand verbunden, aber es geht um das Prinzip."

Wir haben die **Verweigerung der Akteneinsicht** als erheblichen Verstoß gegen die Vorschriften des Datenschutzrechts **beanstandet** und dem Bürger geraten, sein ihm zustehendes Akteneinsichtsrecht nunmehr wahrzunehmen. Daran ist er auch nicht durch die unanfechtbare Entscheidung des Verwaltungsgerichts gehindert, denn er kann jederzeit einen neuen Einsichtsantrag stellen.

Dies sieht der Kreis anders. Der Landrat ließ es in seinem letzten Schreiben an uns bei zwei Zeilen bewenden: „In einem Rechtsstaat ist das Institut der Rechtskraft unantastbar. Vor diesem Hintergrund werde ich Herrn ... keine Akteneinsicht gewähren." Diese Argumentation geht nach unserem Dafürhalten völlig am Problem vorbei. Denn das Verwaltungsgerichtsurteil verneint zwar - zu Unrecht - das Akteneinsichtsrecht des Bürgers, enthält aber natürlich kein Verbot für die Behörde, es zu gewähren, wenn sich herausgestellt hat, daß eine Anspruchsgrundlage übersehen worden ist.

Was ist zu tun?
Der Landrat sollte seine Position noch einmal überdenken und das Recht des Betroffenen auf Akteneinsicht beachten.

4.7 Sozialwesen

4.7.1 Prüfung eines Sozialamtes fördert Umgehung von gesetzlichen Bestimmungen zutage

Ob Sozialhilfeempfänger gleichzeitig Halter von Kraftfahrzeugen sind, darf nur im Einzelfall beim Vorliegen konkreter Anhaltspunkte für Sozialleistungsbetrug ermittelt werden. Ein Sozialamt setzte sich über diese gesetzlichen Bestimmungen hinweg.

Bei der Diskussion über unseren Sozialstaat spielt ein Thema immer wieder eine besondere Rolle: Die rechtswidrige Inanspruchnahme von Sozialleistungen. So hält sich hartnäckig das Bild des Sozialhilfeempfängers, der bequem im eigenen Auto vorfährt, um staatliche Leistungen zu kassieren.

In einer kreisfreien Stadt sollte diesem Gerücht endlich einmal auf den Grund gegangen werden. Bestärkt fühlte man sich durch die letzten Änderungen der Sozialhilfevorschriften, die die unrechtmäßige Inanspruchnahme sozialer Leistungen eindämmen sollen und deshalb zahlreiche neue Datenerhebungs- und -übermittlungsvorschriften enthalten. Der Gesetzgeber läßt einen automatisierten **Datenabgleich** allerdings nur bei Vorliegen **konkreter Anhaltspunkte** zu. Trotzdem übergab das Sozialamt der Zulassungsstelle eine Liste mit den Namen, Vornamen und Adressen aller volljährigen Hilfeempfänger (ca. 4 500). Die Angestellten der Zulassungsstelle waren nun mehrere Tage damit beschäftigt, einzeln zu überprüfen, welcher Sozialhilfeempfänger als Halter eines Pkw eingetragen war. Dies traf bei 546 Personen zu. Bei wie vielen Fällen aber tat-

sächlich Sozialleistungen zu Unrecht gezahlt worden sind, stand bei Fertigstellung dieses Berichts noch nicht fest.



Die **Übermittlung** der Daten von allen 4 500 Hilfeempfängern durch das Sozialamt an die Zulassungsstelle war **rechtswidrig** und mußte von uns beanstandet werden. Denn der Sache nach wurden hier die Bestimmungen umgangen, die einen automatisierten Abgleich nicht zulassen.

4.7.2 Weitergabe einer Telefonnummer durch das Jugendamt mit fatalen Folgen

Eine Mitarbeiterin des Jugendamtes wollte gefällig sein und gab die Telefonnummer einer getrennt lebenden Ehefrau an den Ehemann weiter. Dies hatte zur Folge, daß die Frau ihre Wohnung verlassen und sich wochenlang verborgen halten mußte.

Weil sie von ihrem getrenntlebenden Ehemann erheblich bedroht wurde, war eine Petentin umgezogen, hatte sich eine neue Telefonnummer geben lassen und eine Auskunftssperre beim Melderegister beantragt. Dennoch teilte die Sachbearbeiterin des zuständigen Jugendamtes dem Ehemann die neue Telefonnummer aus Gefälligkeit mit. Dieser terrorisierte die Petentin nun nicht nur mehrmals täglich mit Anrufen, sondern er zeigte solange Fotos seiner Frau in ihrem Wohnort, den er anhand der Vorwahl ausfindig gemacht hatte, herum, bis er ihre neue Adresse ausfindig gemacht hatte. Anschließend suchte er sie auf, um sie erneut zu bedrohen. Mehrfach mußte die Polizei gerufen werden, weil er sich weigerte, die Wohnung zu verlassen. Die Petentin und ihr Sohn verbrachten zwei Tage beim Kinderschutzbund. Danach war die Petentin ohne feste Bleibe, da sie sich nicht mehr in ihre Wohnung zurücktraute.

Entgegen der Annahme des Jugendamtes ist auch die **Telefonnummer** ein **Sozialdatum,** das nur dann übermittelt werden darf, wenn eine gesetzliche Befugnis vorliegt oder die Betroffene eingewilligt hat. Beides war hier nicht der Fall.



Die Übermittlung war daher unzulässig und stellte einen **Verstoß gegen das Sozialgeheimnis** dar, den wir beanstandet haben. Auskünfte über den Aufenthaltsort von Personen dürfen grundsätzlich nur von den Meldebehörden erteilt werden, denn nur dort sind evtl. Auskunftssperren vermerkt.

Was ist zu tun?

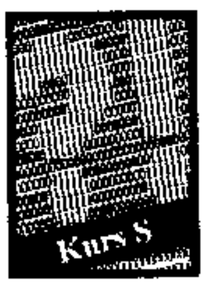
Die Behörde sollte versuchen, den entstandenen Schaden wiedergutzumachen.

4.7.3 Unbefugte Übermittlung von Sozialdaten an einen Zahnarzt

Das Sozialamt darf Ärzte nicht darüber unterrichten, daß Antragstellern die Übernahme von Kostenanteilen im Rahmen der Krankenhilfe abgelehnt worden ist.

Ein Kreissozialamt, das einen Antrag auf Übernahme der Restkosten einer Zahnbehandlung abgelehnt hatte, übersandte eine **Durchschrift** des Bescheides dem behandelnden **Zahnarzt,** der den Heil- und Kostenplan erstellt hatte, **zur Kenntnisnahme** und war verunsichert, als der Antragsteller sich hierüber beschwerte. Im Rahmen unserer Beratung haben wir folgende Position vertreten:

In der Übersendung einer Durchschrift des Ablehnungsbescheides an den behandelnden Zahnarzt lag in der Tat eine **unzulässige** Übermittlung von Sozialdaten vor. Zwischen dem Sozialamt und dem behandelnden Zahnarzt bestanden nämlich überhaupt keine rechtlichen Beziehungen. Es hätte somit der ausdrücklichen Einwilligung des Betroffenen bedurft. Das Kreissozialamt hat diese durch die standardisierte Schweigepflichtentbindungsklausel im Antragsformular des Sozialhilfeträgers als gegeben angesehen. Diese Einwilligung gestattet jedoch lediglich dem Arzt, Auskunft über Fakten zu erteilen, die der ärztlichen Schweigepflicht unterliegen, dem Sozialamt entsteht daraus keinerlei Auskunftsrecht.



4.7.4 Hilfeempfänger bloßgestellt

Das Sozialamt darf nicht über den Kopf der Hilfeempfänger hinweg mit Dritten in Kontakt treten.

Ein **Sozialhilfeempfänger** erhielt vom Sozialamt Eingliederungshilfe zum Besuch einer beruflichen Fachschule. Diese Schule befand sich nicht an seinem Wohnort. Weil der Petent nicht erreichbar war, ließ ihm das Sozialamt seiner Heimatgemeinde wiederholt telefonisch **Nachrichten über die Fachschule** zukommen, z.B. daß ein Termin zwecks Besichtigung des Möbellagers zu vereinbaren sei. Daneben wurden Anfragen an die Schule gerichtet, die zwar abstrakt formuliert waren, bei denen jedoch ein Rückschluß auf den Hilfeempfänger ohne weiteres möglich war. Hierüber beschwerte er sich zu Recht.

Die über die Schule geleiteten Benachrichtigungen stellen eine unbefugte Übermittlung von Sozialdaten dar. Die Unterrichtung hätte durchaus auf schriftlichem Wege erfolgen können. Die **Mitteilungen** waren als unbefugte Weitergabe von Sozialdaten **zu beanstanden**.

Bei der Prüfung von Sozialhilfeakten ergab sich ferner, daß **Auskünfte bei Dritten** zur Klärung bestimmter Zweifelsfragen ohne Kenntnis der Betroffenen eingeholt wurden. Fragt das Sozialamt bestimmte Informationen über jemanden ab, so ist damit gleichzeitig die Offenbarung der Tatsache verbunden, daß diese Person mit dem Sozialamt in Kontakt steht. Bereits dies fällt unter das Sozialgeheimnis. Meist ist jedoch der Datenumfang wesentlich größer. Beantragt z.B. jemand einen Zuschuß zu seiner Hausratversicherung, so wird durch die Nachfrage beim Versicherer, welche Beträge für die einzelnen Risikenanzusetzen sind, der Gesamtumfang des Antrags auf Sozialleistung dem Versicherer gegenüber deutlich gemacht. Derartige Vorgehensweisen sind **ausschließlich mit Einverständnis des Betroffenen zulässig**. Wir haben deshalb Beanstandungen ausgesprochen und die Sozialämter darauf hingewiesen, daß die Einverständniserklärungen der Hilfeempfänger in der Akte zu dokumentieren sind.



Was ist zu tun?
Die Sozialämter sollten sich konsequenter an das Gebot halten, Daten zuallererst beim Betroffenen zu erheben.

4.7.5 Weitergabe von Sozialdaten an Wohnungsbaugesellschaften

Das Sozialamt darf Wohnungsbaugesellschaften keine Listen von wohnungssuchenden Sozialhilfeempfängern ohne deren Einwilligung übermitteln.

Eine Sozialhilfeempfängerin beschwerte sich darüber, daß das Sozialamt Wohnungsbaugesellschaften Listen von wohnungssuchenden Sozialhilfeempfängern zugesandt habe, in denen auch ihr Name und ihre Adresse enthalten seien. Das Sozialamt erklärte dazu, die betroffene Hilfeempfängerin wohne in einer zu teuren Wohnung, und die Stadt habe Belegungsrechte nach dem Wohnungsbindungsgesetz für Wohnungen der fraglichen Wohnungsbaugesellschaft.

Alle Daten über Sozialhilfeempfänger, also auch Name, Anschrift sowie Angaben zum Familienstand, unterliegen dem Sozialgeheimnis und dürfen Dritten nur offenbart werden, soweit hierfür eine spezielle gesetzliche Befugnis oder die Einwilligung der betroffenen Hilfeempfänger besteht. Die Übermittlung von Sozialdaten an private Wohnungsbaugesellschaften war nicht zulässig.

Das Sozialamt kann nämlich von Hilfeempfängern verlangen, daß diese



selbst die erforderlichen Maßnahmen ergreifen, um die Mietkosten zu senken. Daraus folgt, daß das Sozialamt die Hilfeempfänger auffordern kann, sich bei den konkret benannten Wohnungsbaugesellschaften, für die die Stadt Belegungsrechte hat, zu bewerben und Nachweise über die erfolgte Bewerbung vorzulegen.

4.8 Gesundheitswesen

4.8.1 Prüfung der Kassenärztlichen Vereinigung Schleswig-Holstein

Abrechnungsdaten werden bei der Kassenärztlichen Vereinigung zu lange gespeichert. Bei der Vernichtung von Datenträgern konnten Verbesserungen des Verfahrens erreicht werden.

Gegenstand einer Prüfung bei der Kassenärztlichen Vereinigung waren die „routinemäßigen" Datenflüsse von den Ärzten zur Vereinigung und von dort zu den Krankenkassen. Zum Prüfungszeitpunkt erhielt sie noch die Krankenscheine bzw. Disketten zur Abrechnung der Honorare des abgelaufenen Quartals. Das neue automatisierte Abrechnungsverfahren unter Verwendung des sog. ICD-Schlüssels war noch nicht realisiert (vgl. Tz. 4.8.2).

Die Abrechnungsdaten der Ärzte werden **versichertenbeziehbar zehn Jahre** in einer automatisierten Datei **gespeichert**. Diese Speicherungsdauer wird damit begründet, daß es in den Abrechnungen immer wieder zu nachträglichen Korrekturen, z.B. bei unzulässigen Kombinationen von Gebührenordnungsnummern, komme. Hierüber seien langwierige Prozesse zwischen den jeweils betroffenen Ärzten und der Kassenärztlichen Vereinigung zu führen. Es werden allerdings derzeit nicht nur solche Honorarabrechnungsdaten dauerhaft aufbewahrt, bei denen die Ärzte Widerspruch eingelegt haben, sondern der gesamte Datenbestand.

Stichwort Kassenärztliche Vereinigung
Die Kassenärztliche Vereinigung hat der Sozialgesetzgeber als Bindeglied zwischen den Krankenkassen und den Vertragsärzten (Kassenärzten) geschaffen. Sie hat als Körperschaft des öffentlichen Rechts unter anderem die Aufgabe, den Krankenkassen gegenüber zu gewährleisten, daß die Vertragsärzte richtig abrechnen. Die Ärzte rechnen gegenüber der Kassenärztlichen Vereinigung ab, die die Abrechnungsunterlagen prüft und an die Kassen weiterleitet.
Bei den Zahnärzten hat die Kassenzahnärztliche Vereinigung die gleichen Aufgaben.

Nach dem Sozialgesetzbuch V sind alle Daten mit Ausnahme der Angaben über Leistungsvoraussetzungen spätestens nach zwei Jahren zu löschen. Die Aufbewahrungsfrist beginnt mit dem Ende des Geschäftsjahres, in dem die Leistungen gewährt oder abgerechnet wurden. Lediglich in arztbezogener Form dürfen die Daten bis zu zehn Jahre aufbewahrt werden. Die bisherige Speicherpraxis war deshalb zu beanstanden.

Sämtliche **Disketten** mit den Abrechnungsdaten der Ärzte **sowie** sämtliche **Ausdrucke** der Abrechnungsunterlagen werden von einer **privaten Firma** vernichtet. Der Vertrag zur Übernahme und Vernichtung der aus-

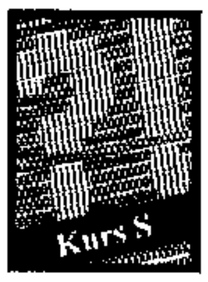
gesonderten Unterlagen sieht vor, daß die Firma das gesamte Material - ohne vorherige Einsichtnahme - entsprechend den Bestimmungen des Landesdatenschutzgesetzes vernichtet. Die Kassenärztliche Vereinigung erhält abschließbare Sicherheitsbehälter, die dann später von der Firma zur Vernichtung abgefahren werden. Für jede Partie bekommt sie eine Vernichtungserklärung.

Bei den zu vernichtenden Daten handelt es sich fast ausschließlich um Unterlagen, die dem **Sozial-** und dem **Patientengeheimnis** unterliegen. Die externe Vernichtung von Datenträgern stellt eine Auftragsdatenverarbeitung im Sinne des § 80 Sozialgesetzbuch X dar, mit der eine **Privatfirma** nur betraut werden darf, wenn

- beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder

- die übertragenen Aufgaben beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfaßt.

Für beides sind im Rahmen der Prüfung keine Anhaltspunkte gefunden worden. Es ist der Kassenärztlichen Vereinigung zuzumuten, die Disketten zunächst unleserlich zu machen und erst dann zur weiteren Vernichtung an die Firma zu geben. Bezüglich der papierenen Unterlagen wäre es durchaus möglich, sie unter Aufsicht eines Mitarbeiters der Kassenärztlichen Vereinigung durch den externen Unternehmer vernichten zu lassen.



Da außerdem die Auftragserteilung bei der Aufsichtsbehörde nicht angezeigt worden war, haben wir die Auftragsdatenverarbeitung **beanstandet**. Die geprüfte Stelle wird das Verfahren entsprechend ändern.

4.8.2 Datenaustausch zwischen Kassenärztlichen Vereinigungen und Krankenkassen im Streit

Die Einführung moderner Technik zur Abrechnung kassenärztlicher Leistungen darf nicht zum „gläsernen Patienten" führen. Wie dies eindeutig sichergestellt werden kann, wird derzeit noch diskutiert.

In seinem Bestreben, Kosten zu sparen, hat der Gesetzgeber auch das Abrechnungsverfahren in der kassenärztlichen Gesundheitsversorgung grundlegend neu organisiert. Bisher wurden die Krankenscheine quartalsweise gebündelt an die Kassenärztlichen Vereinigungen übergeben und von dort nach Prüfung und Abrechnung an die Krankenkassen weitergereicht. Nunmehr ist ein **automatisiertes Verfahren** geplant. Die Einzelheiten darüber regelt ein Vertrag zwischen den Kassenärztlichen Vereinigungen und den Krankenkassen.

Vorgesehen ist, daß die Abrechnungsdaten unter Verwendung des **ICD-10** in maschinenlesbarer Form übermittelt werden sollen. In der Öffentlichkeit ist Kritik am ICD-10 laut geworden, weil er einerseits sehr präzise Angaben vorsieht, so daß er dazu verleiten könnte, mehr Daten als notwendig zu übermitteln, andererseits wiederum zu ungenau ist, um die spezifischen Besonderheiten des Einzelfalles zu erfassen. Kritisch angemerkt wurde auch, daß der ICD-10 eine Reihe von Datenfeldern vorsieht, in denen Ursachen und Begleiterscheinungen von Krankheiten erfaßt werden können. Zum Teil handelt es sich dabei um intime Angaben, die allenfalls für den Arzt bestimmt sind, nicht aber für Abrechnungszwecke. Inzwischen wurde entschieden, die Anwendung des ICD-10 zunächst zwei Jahre zu verschieben, bis die Zweifelsfragen geklärt sind.

Stichwort ICD-10
(International Code of Diseases)
Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme, 10. Revision. Der ICD-10 ist von der Weltgesundheitsorganisation (WHO) erarbeitet worden und dient der Darstellung aller möglichen Krankheitsbilder mit Hilfe eines vierstelligen Codes.
Beispiel: Grippe = J 11.0

Viele Menschen haben sich an uns gewandt und ihre Sorge vor einem **automatisiert erstellten Gesundheitsprofil** geäußert. Die Datenschutzbeauftragten haben erreicht, daß die Kassen die Behandlungsdaten nur **ohne Patientenbezug** erhalten. Die Ärzte übermitteln patientenbezogene Behandlungsdaten lediglich an die Kassenärztlichen Vereinigungen. Diese fungieren als „Clearing-Stellen". Sie trennen nach der Abrechnung der ärztlichen Leistungen die Personendaten von den Behandlungsdaten und leiten diese getrennt weiter. Die Krankenkassen erhalten in getrennten und unterschiedlichen Dateien auf der einen Seite nur den Namen des Patienten sowie dessen Versicherungsnummer, damit sie prüfen können, ob der Behandelte bei ihnen überhaupt versichert ist. Davon völlig losgelöst erhalten sie anonymisiert die Leistungen je Behandlungsfall. Eine Wiederzusammenführung der Daten ist ihnen per Gesetz verboten.

Diese Sicherungen gehen den **Zahnärzten** noch nicht weit genug. Sie meinen, aufgrund der Besonderheiten eines menschlichen Gebisses sei es den Kassen relativ leicht möglich herauszufinden, welche zahnärztliche Behandlung dem einzelnen Versicherten zuzurechnen sei. Auch aus den übrigen Daten lasse sich nach ihrer Auffassung eine Personifizierung mit mathematischen Methoden durchaus herbeiführen. Darüber hinaus bestreiten sie die Befugnis der Krankenkassen, die Abrechnung des Zahnarztes nochmals zu überprüfen. Dies sei allein Aufgabe der Kassenzahnärztlichen Vereinigung. Demzufolge ist der vom Gesetzgeber vorgesehene Vertrag über einen automatisierten Datenaustausch zwischen den Kassenzahnärztlichen Vereinigungen und den Krankenkassen bisher nicht zustande gekommen. In einem angestrengten **Schiedsverfahren** ist die Kassenzahnärztliche Bundesvereinigung unterlegen.

Auch aus unserer Sicht ist die Argumentation der Kassenzahnärztlichen Vereinigungen nicht von der Hand zu weisen, soweit sie darauf pochen, daß nur die zu Abrechnungszwecken erforderlichen Daten an die Kassen übermittelt werden dürfen. Fest steht sicherlich, daß die Krankenkassen alle Daten erhalten müssen, die sie benötigen, um Leistungen korrekt erbringen zu können und die vertragsärztliche Versorgung sicherzustellen. Allerdings bedarf es noch der vertieften Diskussion, in welchem Umfang die Nachprüfungsbefugnis der Kassen besteht und welches Datenprofil dafür tatsächlich notwendig ist. Ob dazu auch der Name des behandelnden Zahnarztes sowie gewisse Einzelheiten der Gebißbehandlung gehören müssen, wird derzeit diskutiert.

Wir haben überdies angeregt zu prüfen, in welchem Umfang das gesetzliche Verbot, die Daten bei den Kassen wieder patientenbezogen zu machen, durch technisch-organisatorische Maßnahmen abgesichert werden kann. Die Gespräche mit der Kassenzahnärztlichen Vereinigung und den Krankenkassen unter Beteiligung des Sozialministeriums waren bei der Fertigstellung dieses Berichts noch nicht abgeschlossen.

4.8.3 Vergabe von Schreibarbeiten an Externe durch öffentliche Krankenhäuser

Krankenhäuser dürfen keine Arztbriefe in Heimarbeit durch Aushilfsschreibkräfte fertigen lassen, wenn die Patienten nicht ausdrücklich eingewilligt haben.

Eine Patientin mußte feststellen, daß ihre Bekannte nähere Kenntnis über ihre gesundheitlichen Leiden hatte. Auf Rückfrage stellte sich heraus, daß diese Informationen aus ihrem Freundeskreis stammten. Nochmalige Nachfragen ergaben, daß die **Krankenberichte** der Petentin von **Privatpersonen in Heimarbeit** außerhalb des Krankenhauses geschrieben wurden.

Dazu teilte uns das Krankenhaus mit, Arztbriefe würden überwiegend vom medizinischen Schreibdienst des Hauses angefertigt. Zum Abbau von Arbeitsspitzen und zur Überbrückung von Ausfällen würden aber auch Mitarbeiterinnen des hauseigenen Schreibdienstes, die sich im Erziehungsurlaub befänden oder nur in Teilzeit arbeiteten, nebenberuflich eingesetzt. Außerdem habe man überdies auch Arbeiten an private Schreibdienste vergeben.

Eine Weitergabe von Patientendaten an **externe Schreibbüros** bedarf der Einwilligung der betroffenen Patienten: Mitarbeiter von externen Schreibbüros können nicht als ärztliches Hilfspersonal angesehen werden,

- weil kein arbeitsrechtliches Verhältnis zwischen Schreibkraft und Krankenhausträger vorliegt und folglich
- ein direktes Direktions- und Weisungsrecht und somit eine unmittelbare Einflußnahme und Kontrolle des Arztes auf die Schreibarbeiten nicht möglich ist.

Soweit das Krankenhaus Schreibarbeiten an **angestellte Schreibkräfte** in Heimarbeit vergibt, sieht die rechtliche Beurteilung anders aus: Hier ist davon auszugehen, daß die Schreibkräfte als ärztliches Hilfspersonal anzusehen sind. Hier stellt sich jedoch die Frage, ob das Krankenhaus die nach dem Landesdatenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen treffen kann, um die erforderliche Datensicherheit zu gewährleisten. Dies dürfte im häuslichen Bereich, zu dem der Dienstherr keinen Zugang hat, kaum möglich sein.

Wie sollte das Krankenhaus in der Lage sein,

- Unbefugten den Zugang zu den Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle),
- zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert, gelöscht oder entwendet werden können (Datenträgerkontrolle),
- die unbefugte Speicherung sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
- zu gewährleisten, daß überprüft und festgestellt werden kann, an wen wann und welche personenbezogenen Daten übermittelt worden sind (Übermittlungskontrolle),
- zu gewährleisten, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert, gelöscht oder entwendet werden können (Transportkontrolle)?

Die Vergabe von Schreibarbeiten an externe Schreibbüros war also eine unbefugte Offenbarung von Patientendaten und somit **förmlich zu beanstanden**.

Auch die Vergabe von Schreibarbeiten an angestellte Schreibkräfte in Heimarbeit war im konkreten Fall als Verstoß gegen das Landesdaten-

schutzgesetz zu beanstanden, da die erforderlichen organisatorischen und technischen Sicherheitsmaßnahmen weder angeordnet noch getroffen waren. Dies hat der Fall der Petentin deutlich gezeigt. Die Klinik hat inzwischen die **Konsequenzen gezogen** und die Vergabe von Schreibarbeiten an private Schreibbüros sowie an Mitarbeiterinnen in Heimarbeit eingestellt.

4.8.4 Chipkarten im Gesundheitswesen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die datenschutzrechtlichen Mindestanforderungen an Verfahren unter Einsatz von Chipkarten im Gesundheitswesen festgelegt.

Derzeit werden in mehreren Ländern Modellversuche und Pilotprojekte mit **Chipkarten im Gesundheitswesen** durchgeführt. Die Bandbreite reicht von **allgemeinen Patientenkarten**, die an möglichst viele Patienten/Versicherte ausgegeben werden, die eine Vielzahl von Krankheitsdaten enthalten und die von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z.B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin) bis zu **krankheitsspezifischen Karten** für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z.B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Stichwort Chipkarten
Es handelt sich um Plastikkarten in der Größe von Scheckkarten mit einem eingeschweißten Prozessor (Rechner) und einem kleinen Datenspeicher. Steckt man sie in ein Schreib-/Lesegerät, erhält man einen vollwertigen PC. Auf einem Chip kann man heute schon bis zu 32 DIN A4 Seiten Text speichern.

Nach Auffassung der Datenschutzbeauftragten muß der **Betroffene** sich **frei** für oder gegen eine Chipkarte **entscheiden** können. Dies umfaßt die Entscheidung,

- **ob** Daten auf einer Chipkarte gespeichert werden,
- **welche** der Gesundheitsdaten auf die Karte aufgenommen werden,
- **welche** Daten auf der Karte wieder **gelöscht** werden,
- **ob** die Karte bei einem Arztbesuch bzw. Apothekenbesuch **vorgelegt** wird und
- **welche Daten** im Einzelfall **zugänglich** gemacht werden.

Ein **Widerruf** der Entscheidung muß ohne Nachteile für den Betroffenen möglich sein.

Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Dem Staat kommt hier nach Auffassung der Datenschutzbeauftragten die Rolle zu, Freiheitsrechte zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung des Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Kartennutzern (z.B. durch Bonuspunkte) bzw. von Kartenverweigerern eingeschränkt werden.

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen auch nicht schlechter gestellt werden als im konventionellen Verfahren. Insbesondere das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. **Verkürzte Darstellungen** medizinischer Sachverhalte auf der Chipkarte - z.B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität der Therapie führen. Der Patient muß auch weiterhin die Möglichkeit des individuellen Dialogs wählen können. Dies schließt die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. So sind Daten auf der Chipkarte so zu ordnen, daß z.B. beim Zahnarzt die gynäkologische Behandlung geheimbleiben kann.

Zur Sicherstellung der Integrität und Authentizität der Daten sind **kryptographische Verfahren** sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche vorzusehen.

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung **neuer zentraler Dateien** von Patientendaten bei Kassenärztlichen Vereinigungen, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen.

Der **Karteninhaber** muß das **Recht** und die Möglichkeit haben, seine auf der Chipkarte gespeicherten **Daten vollständig zu lesen.**

All diese Voraussetzungen für einen gefahrlosen Einsatz von Chipkarten lassen sich **nicht allein** durch die **Einwilligung** der Betroffenen schaffen. Ergänzend sind gesetzliche Regelungen zur Sicherung der Rechte von Patienten und Ärzten notwendig. Ebenso muß der Gesetzgeber den

Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung tragen.

Dies mag folgendes Beispiel verdeutlichen: Die Schutzgemeinschaft für allgemeine Kreditsicherung (**SCHUFA**), bei der praktisch alle Personen registriert sind, die Konsumentenkredite in Anspruch nehmen, erteilt jährlich in mehr als 500 000 Fällen den Betroffenen schriftlich Auskunft darüber, welche Daten über sie gespeichert sind. In den seltensten Fällen geschieht das, weil der Betroffene Zweifel an der Richtigkeit der Daten hat. In der Regel benutzt man eine solche Selbstauskunft, um dem künftigen Arbeitgeber oder Vermieter geordnete finanzielle Verhältnisse nachzuweisen. Einige „schwarze Schafe" verlangen solche Nachweise. In den meisten Fällen werden sie aber freiwillig und unaufgefordert vorgelegt, fast 500 000-mal jährlich! Man stelle sich vor, die Mehrzahl der Bundesbürger würde eine Gesundheitschipkarte bei sich tragen, deren Inhalt man selbst jederzeit ausdrucken könnte. Wie groß wäre wohl die Verlockung, der Bewerbung nicht nur die Schufa-Auskunft, sondern auch ein solches Gesundheitszeugnis beizufügen? Anders gefragt: Welche Chance hätte wohl der Bewerber um einen Arbeitsplatz, der weder das eine noch das andere unaufgefordert vorlegt, wenn die Mehrzahl der Mitbewerber dies tut? Wer würde da nicht gesundheitliche und/oder finanzielle Probleme vermuten?

Was ist zu tun?
Alle, die an Chipkartenprojekten im Gesundheitsbereich arbeiten, sollten die Empfehlungen der Datenschutzkonferenz berücksichtigen.

4.9 Kultusbereich

4.9.1 Automatisiertes Schulverwaltungssystem für die Beruflichen Schulen

Das Land fördert die Einführung eines Schulverwaltungssystems für Berufsschulen, in dem neben den personenbezogenen Schülerdaten auch Lehrerpersonaldaten verarbeitet werden sollen. Unsere Verbesserungsvorschläge wurden berücksichtigt.

Wir haben auf Wunsch des Bildungsministeriums das geplante Schulverwaltungsprogramm „WinSchool" datenschutzrechtlich begutachtet und dabei Abweichungen vom Datenkatalog des Schulgesetzes festgestellt. Da es sich zudem um ein vernetztes Verfahren handelt, haben wir auf die erhöhten Anforderungen hinsichtlich der **Datensicherheit** hingewiesen und entsprechende Vorschläge gemacht. Unsere Hinweise wurden in „WinSchool" berücksichtigt.

Das Bildungsministerium hat im Zusammenhang mit der Einführung des Schulverwaltungsprogrammes eine **Rahmendienstvereinbarung** mit den zuständigen Gewerkschaften geschlossen. Diese sieht u.a. Qualifizierungs- sowie Aus- und Weiterbildungsmaßnahmen für die zukünftigen Benutzer dieses Systems vor. Deshalb führt die DATENSCHUTZ-AKADEMIE gemeinsam mit dem Landesinstitut Schleswig-Holstein für Praxis und Theorie der Schule (IPTS) Kurse für zukünftige Anwender dieses Programmes durch.



4.9.2 Kosten für die Datensicherheit treffen Schulträger

Soll ein Schulgebäude nach Unterrichtsschluß für andere Zwecke genutzt werden und ist damit ein unbeaufsichtigter Zugang zu Räumlichkeiten der Schulverwaltung möglich, müssen die erforderlichen Datensicherheitsmaßnahmen getroffen werden, um zu verhindern, daß schulfremde Personen Zugang zu personenbezogenen Daten der Schüler und Lehrer erhalten. Dies ist Sache des Schulträgers.

Rektoren verschiedener Schulen haben sich mit der Frage an uns gewandt, ob die Schulträger verpflichtet seien, die Kosten für Schlösser zu den Lehrerzimmern zu tragen, wenn nach Unterrichtsschluß Kurse der **Volkshochschulen im Schulgebäude** stattfänden. Die Kursleiter hätten Eingangsschlüssel bekommen, um den Kursteilnehmern den Zugang zum Gebäude zu ermöglichen. Mit Hilfe dieser Schlüssel könnten auch Räumlichkeiten aufgeschlossen werden, in denen personenbezogene Daten der Schüler und Lehrer verwahrt würden.

Nach dem Schulgesetz trägt die **Schulleitung** die **Verantwortung** für die Verwaltung der Schule und damit auch für den Schutz personenbezogener Daten der Schüler sowie der Lehrer. Die erforderlichen und angemessenen Datensicherheitssmaßnahmen sind von den Schulträgern zu realisieren. Daraus folgt auch die Verpflichtung, die erforderlichen finanziellen bzw. Sachmittel zur Verfügung zu stellen.

Was ist zu tun?
Die Schulträger müssen die Kosten für erforderliche und angemessene Datensicherheitsmaßnahmen übernehmen.

4.9.3 Datenschutzverordnung zum Schulgesetz läßt nach wie vor auf sich warten

Die Datenschutzverordnung zum Schulgesetz ist überfällig. Ein vom Bildungsministerium im Laufe des Jahres vorgelegter Entwurf war unzulänglich. Wir haben konkrete Vorschläge zur Verbesserung gemacht.

Auch fünf Jahre nach Inkrafttreten des neuen Schleswig-Holsteinischen Schulgesetzes gibt es noch keine **Rechtsverordnung**, die die im Gesetz allgemein gehaltenen Datenverarbeitungsvorschriften konkretisiert. Zu einem ersten, aus unserer Sicht unzulänglichen Entwurf haben wir folgende **Vorschläge** gemacht:

Für den Bereich der **konventionellen Datenverarbeitung** sollten Regelungen getroffen werden über Inhalt und Gestaltung der Schullaufbahnakte, des Schüleraufnahmebogens, der Klassenbücher sowie über Zugangssicherungen zu den gespeicherten Daten. Außerdem ist eine Überarbeitung der Aufbewahrungsregelungen angezeigt.

Zur Regelung der **automatisierten Datenverarbeitung** haben wir u.a. gefordert, klare Bestimmungen zur Abgrenzung zwischen Unterrichts- und Schulverwaltungsprogrammen sowie zu Netzwerken zu treffen und die Schulträger zu verpflichten, für die Schulung der mit Datenverarbeitung beschäftigten Mitarbeiterinnen und Mitarbeiter zu sorgen. Des weiteren sind Regelungen zur Auftragsdatenverarbeitung zu treffen.



Wir hoffen, daß das Bildungsministerium, auch angesichts einer Reihe von Eingaben, die sich über unzulässige Datenverarbeitungen von Schulverwaltungen beklagen (vgl. z.B. Tz. 4.9.4), nunmehr zügig einen Verordnungsentwurf vorlegen wird.

Was ist zu tun?
Die Bildungsministerin sollte die Datenschutzverordnung nunmehr zügig erlassen.

4.9.4 Wenn zu Hause ein Schulverwaltungsprogramm mit echten Schülerdaten getestet wird

Das Schulgesetz verbietet die Verarbeitung von Schülerdaten mit Hilfe elektronischer Datenverarbeitungsanlagen im häuslichen Bereich der Lehrkräfte. Diese Vorschrift wird nicht immer beachtet. Daraus können sich peinliche Folgen ergeben.

Die Schulleiterin einer Grundschule hatte auf ihrem **häuslichen PC** mit einem Schulverwaltungsprogramm eine **Klassenliste erstellt** und an die Schüler **verteilt**. In dieser Liste waren mehr personenbezogene Daten enthalten als abgesprochen. Neben Namen, Vornamen und Telefonnummern enthielt sie auch das Geburtsdatum, den Geburtsort, die Religion und die vollständige Anschrift der Schülerinnen und Schüler. Darüber beschwerten sich die betroffenen Eltern. Bei der Nachprüfung stellte sich heraus, daß vor Ort die einschlägigen Bestimmungen im Schulgesetz nur ansatzweise bekannt waren. Kenntnisse über die Vorschriften des Landesdatenschutzgesetzes und der Datenschutzverordnung fehlten gänzlich. In Erwartung der Anschaffung eines PC für die Schule wurde aber mit Hilfe der Echtdaten in den Sommerferien schon einmal autodidaktisch die Bedienung des Schulverwaltungsprogrammes geübt. Da die Schulleiterin das Programm jedoch noch nicht richtig beherrschte, war es ihr nicht möglich, die Angaben zu Geburtsort und -datum, Konfession und Anschrift der Schüler herauszufiltern. Sie habe sich jedoch nichts weiter dabei gedacht und die Klassenliste in der unzulässigen Form trotzdem verteilt. Dies war zu beanstanden.

Dieser Vorfall zeigt einmal mehr, daß es erforderlich ist, die Beschaffung von EDV-Technologie mit der gleichzeitigen fachlichen und **datenschutzrechtlichen Unterweisung** der Benutzer zu verknüpfen, so wie es das Landesdatenschutzgesetz ausdrücklich fordert.



Die verbreitete Benutzung von PC im häuslichen Bereich der Lehrer führt offenbar zunehmend dazu, daß personenbezogene Schülerdaten entgegen der eindeutigen Vorschrift im Schulgesetz auf Privat-PC verarbeitet werden. Dies scheint gelegentlich sogar mit Kenntnis und Billigung der Schulleitungen zu geschehen.

Was ist zu tun?
Es ist Sache des Bildungsministeriums, auf die Einhaltung dieser Vorschrift hinzuwirken und bei nachgewiesenen Verstößen auch weitergehende Maßnahmen zu ergreifen.

4.9.5 Datenschutz gegenüber Elternvertretern

Die im Schulgesetz festgelegten Beteiligungsrechte der Elternvertreter erfordern eine ausreichende Information über die entscheidungserheblichen Sachverhalte. Dabei sind jedoch im Einzelfalle die berechtigten Interessen von Eltern zu berücksichtigen.

Eine Schulelternbeiratsvorsitzende hatte sich an uns gewandt, weil der Schulleiter Elternvertretern in Einzelfällen die Teilnahme an der Erörterung von Problemen einzelner Schüler verweigert hatte, sofern nicht eine ausdrückliche Genehmigung der betroffenen Eltern vorlag. Die **Schulelternbeiratsvorsitzende** war der Auffassung, daß dies mit den Beteiligungsrechten nach dem Schulgesetz nicht im Einklang stand. Dem haben wir grundsätzlich zugestimmt, da es Aufgabe der Elternvertreter ist, die Eltern gegenüber der Schule zu vertreten und damit als Mittler aufzutreten. Hierzu ist eine **ausreichende Information** der Elternvertreter erforderlich.

Allerdings sind auch Situationen denkbar, in denen in Einzelfällen berechtigte Interessen von Eltern dazu führen müssen, daß dem Elternvertreter keine Einsicht in die Unterlagen gewährt wird (z.B. zur Vermeidung einer Offenbarung „sensibler" Familienverhältnisse gegenüber Nachbarn, abhängigen Mitarbeitern, persönlich verfeindeten Personen). Wir haben gegenüber dem Ministerium angeregt, in solchen Fällen ein **Widerspruchsrecht betroffener Eltern** vorzusehen. Man hat sich unserer Anregung aber unter Hinweis auf die im Schulgesetz verankerten Beteiligungsrechte der Elternvertreter nicht anschließen wollen. Es muß also der Schulleitung überlassen bleiben, im Einzelfall zu entscheiden, ob von Eltern vorgetragene Vorbehalte gegen die Beteiligung der Elternvertreter zu beachten sind.

Was ist zu tun?
Schulleiter sollten im Einzelfall den begründeten Wunsch von Eltern, in ihrem Fall die Elternvertretung nicht zu beteiligen, berücksichtigen.

4.9.6 Zuteilung von Kursplätzen an einer Universität durch den Computer

Die Vergabe von Kursplätzen per Computer setzt voraus, daß Umfang und Verfahren der Verarbeitung von Studentendaten in der Studien- und Prüfungsordnung geregelt sind. Eine Behörde darf sich beim Computereinsatz nicht von einem einzigen Mitarbeiter abhängig machen.

Durch eine Zeitung wurden wir informiert, daß eine Fakultät einer Hochschule ein **EDV-gestütztes Kursvergabesystem** betreibt. Jeder Studierende muß sich über die Terminals im PC-Labor zu den Kursen anmel-

den. Die so gesammelten Daten werden mit der automatisierten Studentendatei des Sekretariats zusammengeführt. Mit Hilfe eines speziellen Programms werden die Kursplätze zugewiesen. Nach Abschluß des Verfahrens werden die Ergebnisse durch Aushang veröffentlicht.

Eine Nachschau vor Ort ergab, daß dieses DV-Konzept zur Verwaltungsvereinfachung von einem einzelnen Mitarbeiter der Fakultät entwickelt worden war. Nur der war in der Lage, die endgültige Auswertung zu starten, ein Vertreter war nicht bestellt. Wir haben die Universität auch darauf hingewiesen, daß bei der automatisierten Verarbeitung von Studentendaten die **technischen und organisatorischen Maßnahmen** zur Datensicherheit zu treffen sind. Hierzu gehört es unabdingbar, daß die fachlichen Vorgaben an Datenverarbeitung schriftlich geregelt sind. Das Verfahren muß getestet und freigegeben und gegen Manipulationen gesichert sein. Wichtig ist außerdem, daß die Betreuung und Handhabung der EDV-Verfahren nicht nur von einer Person wahrgenommen wird, sondern daß ein kompetenter Vertreter vorhanden ist.

Darüber hinaus ergab unsere Nachprüfung, daß zwar nur die nach der Studentendatenverordnung vorgesehenen Daten verarbeitet werden, jedoch fehlt es an einer ausdrücklichen Erlaubnisvorschrift hinsichtlich der Erhebung dieser Daten in der Studien- und Prüfungsordnung zum Zweck der Kursplatzvergabe. Eine ausdrückliche Einwilligung wurde von den Studierenden nicht eingeholt, und diese wurden nicht über die Bedeutung und die näheren Umstände des Verfahrens aufgeklärt. Somit wurden Daten ohne Rechtsgrundlage verarbeitet. Aufgrund unserer Beanstandung hat die Universität damit begonnen, die **Studien- und Prüfungsordnungen** um Datenerhebungsvorschriften zu ergänzen, aus denen genau ersichtlich ist, welche personenbezogenen Daten von den Studenten für welche Zwecke erhoben und weiterverarbeitet werden. Bis zum Inkrafttreten dieser Satzungen werden die Studenten förmlich um das Einverständnis in die EDV-gestützte Kursplatzvergabe und die anschließende Veröffentlichung durch Aushang gebeten und durch ein Merkblatt umfassend über das Verfahren unterrichtet.



4.10 Steuerverwaltung

4.10.1 Endlich Regelungen zur Datensicherheit geschaffen

Das Regelungsdefizit bezüglich der Datensicherheit in den Finanzämtern ist endlich behoben worden. Dabei wurde auch die Verantwortung für unzulängliche technische und organisatorische Gegebenheiten klargestellt.

„Gut Ding will Weile haben" mag der Finanzminister gedacht haben, als er sich fast drei Jahre Zeit nahm, um die von uns im Rahmen einer datenschutzrechtlichen Überprüfung einiger Finanzämter im Jahre 1992 festgestellten Defizite bezüglich der Datensicherheit zu beheben. Über die Gründe für diese Zeitverzögerung ist bereits im 17. Tätigkeitsbericht (Tz. 4.5.1) berichtet worden (Sparsamkeit am falschen Platz und Regelungsunschärfen führten zu Bedenken der Personalräte).

Nunmehr ist endlich Bewegung in die Angelegenheit gekommen. Im November 1995 hat der Finanzminister im Einvernehmen mit dem Hauptpersonalrat **Anweisungen** zur besseren **Sicherung von Akten** und sonstigen **Datenträgern** in den Finanzämtern erlassen, die in mehrfacher Hinsicht bemerkenswert sind.

Da ist zunächst eine Regelung hervorzuheben, die es in dieser Klarheit nach unserer Kenntnis bisher noch in keinem anderen Verwaltungsbereich gibt. Sie lautet: „Für die Einhaltung der Regelungen zum Steuergeheimnis und des Datenschutzes ist jeder Beschäftigte für seinen Bereich verantwortlich. Die persönliche Verantwortung des einzelnen geht allerdings nur so weit, wie auch die erforderlichen Rahmenregelungen für die Einhaltung der Aktensicherheit, die vom Dienstherrn zu schaffen sind (z.B. Abschließbarkeit der Räumlichkeiten), tatsächlich vorhanden sind." Dies bedeutet nichts anderes, als daß bezüglich der Ausgestaltung der konkreten **Datensicherungsmaßnahmen** zunächst **der Dienstherr „am Zuge** ist". Strukturelle Mängel in diesem Bereich können nicht den Mitarbeitern angelastet werden. Sie sind nur dann zur Rechenschaft zu ziehen, wenn sie bestehende Regelungen, Weisungen oder Verbote nicht beachten. Es wird an den Mitarbeitern selbst und an ihren Personalvertretungen liegen, die Behördenleitungen zur Abhilfe zu drängen, wenn technische und organisatorische Gegebenheiten Sicherheitslücken aufweisen.

Die einzelnen Bestimmungen des Erlasses zwingen die Finanzämter, (endlich) dafür zu sorgen, daß

- **Steuerakten** nur in **verschlossenen Räumen** bzw. in **abgeschlossenen Schränken** gelagert werden,

- technische **„Dienstleister"** (Reinigungspersonal, Handwerker, Techni-

ker usw. von Fremdfirmen) **nicht unbeaufsichtigt** in Kontakt mit steuerlichen Unterlagen kommen,

- über den **Verbleib** von Steuerakten, die an andere Stellen weitergegeben werden, **Buch geführt** wird und daß

- **Außendienstmitarbeiter** in die Lage versetzt werden, Steuerakten im häuslichen Bereich und während ihrer Tätigkeit beim Steuerpflichtigen in verschlossenen Behältnissen zu verwahren.

Dies wird sicherlich nicht unerhebliche technische und organisatorische Veränderungen in den meisten Finanzämtern zur Folge haben müssen. Deshalb werden wir uns zu gegebener Zeit durch erneute Stichprobenkontrollen davon überzeugen, daß der nachfolgend beschriebene Sachverhalt (vgl. Tz. 4.10.2) sich möglichst nicht wiederholen kann.

Was ist zu tun?
Die Finanzämter sollten den Erlaß des Finanzministers zügig umsetzen.

4.10.2 Steuerakten von Prominenten gestohlen

Der Diebstahl von Steuerakten Prominenter unterstreicht einmal mehr die Richtigkeit unserer Forderung, daß für Datenbestände, die wie Steuerakten einem besonderen Amtsgeheimnis unterliegen, Sicherungsmaßnahmen zu ergreifen sind, die generell nur durch Anwendung physischer Gewalt zu „durchbrechen" sind.

„Steuerakten von Prominenten gestohlen", so lautete eine Zeitungsmeldung, in der darüber berichtet wurde, daß ein ehemaliger Finanzbeamter die Steuerakten von sieben prominenten Mitbürgern (darunter die eines Staatssekretärs und eines Richters) aus dem Bestand eines Finanzamtes in seinen Besitz gebracht hatte. Seine Motive und seine Vorgehensweise blieben zwar im Dunkeln, auch wurde der Schaden relativ schnell entdeckt, so daß der Täter die Akten wohl noch nicht einmal selbst studiert hatte. Von sicherheitstechnischer Bedeutung ist jedoch der Umstand, daß bei dem Diebstahl **keine physische Gewalt** angewendet wurde. Dies bestätigte im Rahmen unserer Nachforschungen auch das betreffende Finanzamt. Der Täter müsse sich durch kriminelle Energie und Ausnutzung seiner Kenntnisse aus der früheren Zugehörigkeit zum Hause Zugang verschafft haben. Es sei auch möglich, daß er sich in das Gebäude habe einschließen oder aber bereits während seiner Dienstzeit Duplikate von Schlüsseln habe anfertigen lassen. Man habe aufgrund dieses Vorfalls neue Sicherheitsschlösser in die Außentüren und „einige besonders sensible" Bereiche im Gebäude eingebaut.

Welche Rolle bei dem Diebstahl Insiderwissen gespielt hat, ist aus unserer Sicht von untergeordneter Bedeutung. Derartige Kenntnisse können mittels schlichter Beobachtung durch eine Vielzahl von Personen erworben und unkontrolliert weiterverbreitet werden. Für Datenbestände, die wie Steuerakten einem besonderen Amtsgeheimnis unterliegen, ist generell zu fordern, daß eine unbefugte Inbesitznahme stets nur mit Anwendung physischer Gewalt erfolgen kann. **Sicherheitsschlösser** und **Schließanlagen** bieten nur dann ein angemessenes Sicherheitsniveau, wenn nicht besetzte Büroräume auch **tatsächlich verschlossen** werden bzw. wenn die personenbezogenen Unterlagen in verschlossenen Behältnissen verwahrt werden. Sie verlieren ihre Wirkung, wenn z.B. die Sicherheitsschlüssel im Schloß stecken, die Schlüsselkästen für Unbefugte frei zugänglich angebracht sind oder die Schlüssel zu Diensträumen von den Mitarbeitern an sich genommen und unbeaufsichtigt gelassen werden.



Daß gerade Akten von Prominenten entwendet wurden, hat die Bedeutung der Datensicherheit in den Finanzämtern (vgl. Tz. 4.10.1) auch in der Öffentlichkeit besonders plastisch gemacht.

4.10.3 „Versprochen ist versprochen" gilt auch für die Steuerverwaltung

Die Steuerverwaltung ist verpflichtet darauf hinzuweisen, daß Kontonummern, die von Steuerpflichtigen freiwillig zum Zweck der Erstattung von Überzahlungen angegeben werden, bei evtl. Vollstreckungsmaßnahmen als Anhaltspunkte für Pfändungen benutzt werden.

Wer ein Kraftfahrzeug anmeldet, wird vom Finanzamt in der gleichzeitig auszufüllenden Steuererklärung für die Kraftfahrzeugsteuer gebeten, bereits zu Beginn der Steuerpflicht ein **Konto** anzugeben, auf das am Ende der Steuerpflicht ein evtl. **Erstattungsbetrag** überwiesen werden könne. Dieses Ansinnen ist durchaus logisch. Man bezahlt nämlich die Kraftfahrzeugsteuer für ein Jahr im voraus, und es ist höchst unwahrscheinlich, daß man das Auto genau am Kauftag auch wieder veräußert. In der Regel ergibt sich also am Ende der Steuerpflicht eine Überzahlung. Die Finanzämter sind natürlich daran interessiert, diese möglichst kostengünstig von Konto zu Konto und nicht mittels eines teuren Barschecks abzuwickeln. Andererseits ist niemand verpflichtet, ein Konto zu haben bzw. anzugeben. Mithin liegt ein klassischer Fall der **freiwilligen Datenhergabe** im Sinne des Datenschutzrechts vor.

Diese Feststellung spielte eine große Rolle in einem Fall, in dem das betreffende Finanzamt Steuerschulden einer Person durch **Vollstreckungsmaßnahmen** einzutreiben versuchte. Es fand heraus, daß der Steuerschuldner ein Kraftfahrzeug benutzte, befragte das für die Kraftfahrzeug zuständige Finanzamt nach dem dort angegebenen Erstattungskonto und pfändete das auf dem Konto vorhandene Guthaben.

Der Steuerpflichtige machte geltend, dies sei unzulässig. Das Kraftfahrzeugsteuer-Finanzamt hätte den Kollegen des anderen Finanzamtes die Bankverbindung nicht zu Vollstreckungszwecken preisgeben dürfen. Er habe sie nur zu Erstattungszwecken freiwillig offenbart. Demzufolge habe es sich um eine **unzulässige Zweckänderung** gehandelt.

Das Finanzamt und die Oberfinanzdirektion beriefen sich darauf, daß das Steuergeheimnis nicht verletzt worden sei, weil Daten zwischen den verschiedenen Steuerarten ausgetauscht werden dürften. Außerdem seien die Vollstreckungsstellen nach der Abgabenordnung gehalten, zur Vorbereitung der Vollstreckung die Vermögens- und Einkommensverhältnisse zu ermitteln. Die Nutzung der Kontoangaben zu Vollstreckungszwecken sei mithin zulässig.

Auf den ersten Blick möchte man den Steuerbehörden Recht geben. Wo kämen wir denn hin, wenn säumige Steuerzahler die Konten, auf denen sie Geldbeträge „geparkt" haben, auf diese Weise gezielt dem Zugriff der Vollstreckungsbeamten entziehen könnten. Spräche sich diese Möglichkeit herum, fände man unter den Kraftfahrzeugsteuer-Erstattungskonten bald die Nummern vieler „millionenschwerer Sparbücher".

Diese Argumentation greift jedoch zu kurz. Die Kernfrage lautet nämlich: „Ist das Finanzamt an sein Versprechen gebunden, das Konto nur für Erstattungszwecke zu speichern?" Aus datenschutzrechtlicher Sicht ist diese Frage mit einem klaren „Ja" zu beantworten.

Die Zweckbindungsregelungen finden zwar dann ihre Grenzen, wenn eine Rechtsvorschrift eine Verarbeitung zu anderen Zwecken erlaubt oder im Einzelfall zwingend voraussetzt. Auf diesen Umstand sind die **Betroffenen** jedoch **bei der Datenerhebung hinzuweisen**. Das gilt insbesondere dann, wenn sie gebeten werden, die Angaben freiwillig zu machen. Auch das ist im Datenschutzrecht festgeschrieben.

Es mag den Finanzämtern nicht leichtfallen, auf den bundesweit millionenfach benutzten Vordrucken eine entsprechende Formulierung unterzubringen. Bis ihnen dies gelungen ist, gilt jedoch der Grundsatz: „Versprochen ist versprochen." Hierauf haben wir die Oberfinanzdirektion hingewiesen.

Was ist zu tun?
Der Finanzminister sollte auf eine Änderung der Vordrucke hinwirken oder die Finanzämter müssen sich an ihre Zusagen konsequent halten.

4.10.4 Die Freiheit, zu viel Steuern zu zahlen

Auch wenn man zur Abgabe von Steuererklärungen verpflichtet ist, ist die Angabe von steuermindernden Sachverhalten stets freiwillig. Ein Gesellschafter kann durchaus ein Interesse daran haben, daß seine Mitgesellschafter über bestimmte nur ihn betreffende Sachverhalte nichts erfahren.

In vielen Fällen wird man durch das Steuerrecht gezwungen bzw. tut gut daran, gemeinsam mit mehreren Personen eine „**einheitliche**“ **Steuererklärung** abzugeben. Das gilt z.B. für Mitglieder von Personengesellschaften, Grundstücks- und Erbengemeinschaften, aber ebenso, wenn sich Ehegatten zur Einkommenssteuer zusammen veranlagen lassen. Zweifellos ist man auch unter diesen Bedingungen verpflichtet, alle Angaben zu machen, die zur vollständigen Erfassung der steuerpflichtigen Sachverhalte erforderlich sind. Man kann sich nicht darauf berufen, daß aus Gründen des Steuergeheimnisses die anderen „Mitsteuerpflichtigen“ über bestimmte Gegebenheiten nicht informiert werden dürfen.

Gilt dies aber auch für Angaben, die steuermindernden Charakter haben? Diese Frage war zu klären in einem Fall, in dem ein Finanzamt, weil sich die zwei Mitglieder einer Grundstücksgemeinschaft nicht über die Abgabe einer gemeinsamen Erklärung einigen konnten, die Einzelbeträge einfach aus den jeweiligen persönlichen Einkommenssteuererklärungen in ein sogenanntes „gesondertes und einheitliches Feststellungsverfahren“ übernommen hatte. Über die vollständige Erfassung der Einnahmen gab es keinen Streit. Einer der Gesellschafter beklagte sich jedoch darüber, daß auf diese Weise **steuermindernde Ausgaben**, die nur ihm zuzurechnen waren, **dem anderen Mitgesellschafter bekanntgeworden** waren. Hieraus ergäben sich so große zivilrechtliche Probleme, daß er es vorgezogen hätte, auf die steuerliche Berücksichtigung zu verzichten. Er sehe in der Verfahrensweise des Finanzamtes einen **Bruch des Steuergeheimnisses**.

Das Finanzamt rechtfertigte sein Tun mit dem gesetzlichen Auftrag, bei der Steuerfestsetzung „alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände, zu berücksichtigen“. Dem konnten wir uns ebenso wie der Betroffene nicht anschließen. Kein **Steuerpflichtiger** kann verpflichtet werden, steuerliche Vergünstigungen auch tatsächlich in Anspruch zu nehmen. Was für ihn günstig ist, kann er nach seinen eigenen Maßstäben **selbst entscheiden**. Hieraus folgt, daß er in einer Steuererklärung, auch wenn man zu deren Abgabe gesetzlich verpflichtet ist, die Angaben über steuermindernde Sachverhalte und Beträge stets freiwillig erfolgen.

Was ist zu tun?
Die Finanzämter sollten dies künftig beachten.

4.11 Personalwesen

Der richtige Umgang mit Personaldaten bereitet in der Praxis offenbar immer wieder Schwierigkeiten. Das neuen Landesbeamtengesetz bringt endlich Rechtsklarheit.

4.11.1 Verarbeitung von Bewerberdaten im Polizeibereich neu geregelt

Durch eine Eingabe wurden wir darauf aufmerksam gemacht, daß bei der Werbe- und Einstellstelle der Polizei **Daten abgelehnter Bewerber** grundsätzlich für **fünf Jahre** aufbewahrt wurden, obwohl die Löschung solcher Daten verbindlich vorgeschrieben ist, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Unsere Nachforschungen ergaben darüber hinaus weitere Verfahrensmängel. Dies führte dazu, daß die Verarbeitung von Bewerberdaten jetzt durch einen Runderlaß **neu geregelt** wurde. Von Bedeutung sind folgende Festlegungen:

- Zugang zu Einstellungsvorgängen dürfen jetzt nur noch Mitarbeiter erhalten, die für die Bearbeitung des betreffenden Vorgangs zuständig sind.

- Bei der Einstellung dürfen nur solche Bewerbungsunterlagen in die Personalakte übernommen werden, die zur Begründung des Dienstverhältnisses erforderlich sind.

- Eingereichte Unterlagen werden bei Rücknahme der Bewerbung sofort, sonst spätestens mit dem Ablehnungsbescheid, zurückgegeben.

- Die verbleibenden Restvorgänge werden wegen möglicher Rechtsmittelverfahren nach der Entscheidung für ein Jahr aufbewahrt und anschließend vernichtet.

Was ist zu tun?
Die Einstellstelle der Polizei muß ihr Verfahren dem Erlaß anpassen.

4.11.2 Anforderung uneingeschränkter Bundeszentralregisterauskünfte durch die Reaktorsicherheitsbehörde

Mitarbeiter von Firmen, denen der Zutritt zu kerntechnischen Anlagen, wie z.B. Atomkraftwerken, gestattet wird, müssen sich nach den Vorschriften des Atomgesetzes einer Sicherheitsüberprüfung unterziehen. Zuständige Stelle ist in Schleswig-Holstein die Reaktorsicherheitsbehörde. Sie befragt zu diesem Zweck die Verfassungsschutzbehörde über relevante Erkenntnisse sowie das Bundeszentralregister über vorhandene Eintragungen. Zur „Vereinfachung des Verwaltungsverfah-

rens“ wurde bisher der Zentralregisterauszug über die **Verfassungsschutzbehörde** angefordert. Sie leitete den Auszug ihrerseits der Reaktorsicherheitsbehörde zu und bekam dadurch natürlich Eintragungen zur Kenntnis, die sie für die Erfüllung ihrer eigenen Aufgaben gar nicht benötigte.

Wir haben die Reaktorsicherheitsbehörde ersucht, zukünftig alle **Anfragen selbst beim Bundeszentralregister** zu stellen und die Antworten nicht mehr über die Landesverfassungsschutzbehörde leiten zu lassen. Die Reaktorsicherheitsbehörde hat sich unserer Auffassung angeschlossen und das Verfahren entsprechend umgestellt.

4.11.3 Was nicht in die Personalakte gehört

Eine Mitarbeiterin hatte mit einem Dienstwagen die in Ortschaften zulässige Höchstgeschwindigkeit geringfügig überschritten und war dabei in eine Polizeikontrolle geraten. Die **Anhörung im Bußgeldverfahren** richtete sich zunächst gegen den Dienstherrn, da dieser als Halter des Pkw im Zulassungsregister gespeichert war. Natürlich wurde die Anhörung an die betroffene Mitarbeiterin zur Stellungnahme weitergeleitet. Zusätzlich wurde jedoch auch eine Kopie des Anhörungsbogens zu ihrer **Personalakte** genommen, ohne daß sie davon wußte.

In die Personalakte dürfen nur Unterlagen aufgenommen werden, die mit dem Beschäftigungsverhältnis in einem unmittelbaren Zusammenhang stehen. Eine Anhörung in einem Bußgeldverfahren stellt jedoch keine relevante Dienstpflichtverletzung dar. Bei der Nachprüfung der Angelegenheit stellten wir fest, daß sogar „Bestimmungen beim Schwimmen und Baden“ (die Betroffene arbeitete als Erzieherin) und die Anweisung, wie ihr Privat-Pkw auf dem Dienstgelände abgestellt werden müsse, in der Personalakte abgeheftet waren. Die Unterlagen sind auf unsere Beanstandung hin aus der Personalakte entfernt und vernichtet worden.



4.11.4 Jährliche Überprüfung des erhöhten Ortszuschlages nicht erforderlich

Die Zahlung eines erhöhten Ortszuschlages an Mitarbeiter im öffentlichen Dienst ist im wesentlichen von den familiären Verhältnissen abhängig. Eine Überprüfung der Anspruchsvoraussetzungen durch das Landesbesoldungsamt erfolgt in der Regel alle drei Jahre. Davon abweichend müssen jedoch Beschäftigte, die einen erhöhten Ortszuschlag wegen Aufnahme einer Person in die Wohnung erhalten, bereits nach einem Jahr eine sog. **Kinder- und Ortszuschlagserklärung** abgeben. Betroffen von dieser Regelung sind Alleinerziehende - in erster Linie Frauen -, die ein oder mehrere Kinder in ihrem Haushalt betreuen.

Begründet wurde der kürzere Befragungsrhythmus vom **Landesbesoldungsamt** damit, daß „bereits die bisherige Verfahrensweise der rückwirkenden Überprüfung der gesetzlichen Anspruchsvoraussetzungen für ein Jahr in einer nicht unerheblichen Zahl von Fällen die Zahlungsempfängerinnen und Zahlungsempfänger in Beweisnot brachte, da sie die erforderlichen Nachweise nicht mehr besaßen und teils unter großen Schwierigkeiten neu beschaffen mußten".

Diese Begründung kann nicht überzeugen, da jeder Gehaltsempfänger verpflichtet ist, **Veränderungen** in seinen familiären Verhältnissen **selbst rechtzeitig anzuzeigen**, und es hier nur um eine Kontrolle gehen kann, ob die Anzeigepflicht tatsächlich beachtet wurde. Das Landesbesoldungsamt hat nunmehr eingeräumt, daß in Fällen, in denen Kinder unter 16 Jahren betreut wurden, ein Überprüfungszeitraum von drei Jahren ausreicht. Für alle anderen Fallgruppen wird weiterhin ohne Nachweis von „Beweisnotfällen" die jährliche Überprüfung beibehalten.

4.11.5 Was darf der Schulelternbeirat über Fehlzeiten der Lehrer erfahren?

Ein Personalrat im Lehrerbereich legte dar, es sei weitgehend üblich, über die Fehlzeiten von Lehrkräften detaillierte Listen einschließlich der Gründe wie Krankheit, Arztbesuch, Art der Fortbildung, dienstliche und private Beurlaubung mit Erläuterungen zu erstellen und sie in der Schule mit dem Elternbeirat, aber auch öffentlich, zu erörtern oder sogar in öffentlich zugänglichen Vertretungsplänen darzustellen. Dies führe zu Versuchen von Eltern, auf Entscheidungen des Schulleiters Einfluß zu nehmen bzw. zu Animositäten gegenüber einzelnen Lehrkräften.

Wir haben darauf hingewiesen, daß zu den **dienstlichen Daten** über Mitarbeiter öffentlicher Stellen, neben Namen, dienstlicher Telefonnummer, Dienstbezeichnung und die Funktion des Mitarbeiters auch die Tatsache der Teilnahme an einer dienstlichen Fortbildungsmaßnahme oder die Nennung eines sonstigen dienstlich veranlaßten Abwesenheitsgrundes, gehören.

Geschützt und damit dem Informationsanspruch des Schulelternbeirats entzogen sind allerdings Daten, die das **persönliche Verhältnis der Lehrkraft** und anderer Mitarbeiter zu ihrem Dienstherrn berühren oder ihren privaten Bereich betreffen. Daten über Erkrankungen, Arztbesuche oder private Gründe für Beurlaubungen dürfen deshalb grundsätzlich nicht veröffentlicht werden. Auch für eine Weitergabe solcher Daten an den Schulelternbeirat gibt es keine Befugnisgrundlagen. Daraus folgt schließlich auch, daß eine Veröffentlichung privater Fehlgründe auf den schulöffentlich ausgehängten Vertretungsplänen unzulässig ist.

4.11.6 Neues Personalaktenrecht endlich verabschiedet

Bereits seit dem 01.01.1993 hat der Bund im Beamtenrechtsrahmengesetz die Verarbeitung von Personaldaten detailliert geregelt. Nach eingehender Beratung hat nun auch der Landtag das Landesbeamtengesetz an die Maßgaben des Rahmenrechts angepaßt und durch Änderung des Landesdatenschutzgesetzes seine Anwendung auf alle Mitarbeiter des öffentlichen Dienstes in Land und Kommunen erstreckt. Damit ist eine seit mehr als drei Jahren bestehende **Rechtsunsicherheit** im Bereich des Personaaktenrechts endlich **beseitigt**. Für die Betroffenen ist das neue Recht mit wesentlichen Verbesserungen verbunden. Dazu gehören:

Vertraulicher Umgang mit Personalakten

Die vertrauliche Behandlung von Personalakten auch innerhalb der Verwaltung wird besonders herausgestellt. Zur Sicherung der Vertraulichkeit sind organisatorische Regelungen vorgesehen, die den verwaltungsmäßigen Umgang mit Personalakten erheblich beschränken. So dürfen **Personalnebenakten** innerhalb einer Behörde nicht mehr geführt werden. Dabei handelt es sich um Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden. Mit dieser Regelung soll verhindert werden, daß in Fachabteilungen bzw. bei Fachvorgesetzten Zweitakten geführt werden. Personalentscheidungen der Behörde sollen zudem nur noch aufgrund von Daten aus der Originalakte getroffen werden.

Zugang zu Personalakten haben nur noch Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Für Fachvorgesetzte besteht damit keine Möglichkeit mehr, in Personalakten ihrer Mitarbeiter Einsicht zu nehmen. Ggf. sind ihnen die im Einzelfall zur Aufgabenerfüllung erforderlichen Personalaktendaten zur Kenntnis zu geben. Vorgesetzte sollen bei der Wahrnehmung der Fachaufsicht über ihre Mitarbeiter nicht durch Kenntnisse aus der Personalakte beeinflußt werden.

Erweitertes Auskunfts- und Akteneinsichtsrecht für Betroffene

Bisher hatten Mitarbeiter lediglich das Recht auf Einsicht in ihre vollständige Personalakte. Andere Unterlagen, in denen Personaldaten über sie gespeichert wurden, blieben ihnen in der Regel verschlossen. Nunmehr verfügen Mitarbeiter über ein generelles **Recht auf Einsicht** in alle Akten, die personenbezogene Daten über sie enthalten und für ihr Dienst- oder Arbeitsverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Ist eine Einsichtnahme nicht möglich, weil die Daten der Betroffenen mit Daten Dritter oder mit geheimhaltungsbedürftigen Daten verbunden sind, müssen vom Dienstherrn entsprechende Auskünfte erteilt werden.

Anspruch auf Entfernung von Unterlagen aus Personalakten

Erstmalig werden „Verjährungsfristen" für die Aufbewahrung belastender Unterlagen in Personalakten eingeführt. Der vom Bundesverwaltungsgericht entwickelte Vollständigkeitsgrundsatz (Unterlagen, die einmal rechtmäßig in die Personalakte aufgenommen wurden, dort wegen der notwendigen Schlüssigkeit der Akte dauerhaft gespeichert bleiben) für Personalakten verliert damit seine Gültigkeit.

Unterlagen über Beschwerden, Behauptungen und Bewertungen, auf die die Tilgungsvorschriften des Disziplinarrechts keine Anwendung finden, sind künftig,

- falls sie sich als unbegründet oder falsch erwiesen haben, mit Zustimmung des Betroffenen unverzüglich aus der Personalakte zu entfernen und zu vernichten,

- falls sie für den Betroffenen ungünstig sind oder ihm nachteilig werden können, auf seinen Antrag nach drei Jahren zu entfernen und zu vernichten; ausgenommen sind dienstliche Beurteilungen.



Angesichts dieses Entfernungsanspruchs, der auch für Unterlagen aus Zeiten vor Inkrafttreten der Neuregelung geltend gemacht werden kann, werden sich viele Mitarbeiter überlegen, ob sie dies zum Anlaß nehmen, einmal ihre Personalakte durchzusehen.

Was ist zu tun?
Die Personaldaten verarbeitenden Stellen haben rechtzeitig den erheblichen Schulungs- und Aktenbereinigungsaufwand einzuplanen.

4.11.7 Aktenordnung für den Personalrat

Ist die Kenntnis personenbezogener Daten nach Abschluß eines Vorgangs zur Aufgabenerfüllung der datenverarbeitenden Stelle nicht mehr erforderlich, schreibt das Landesdatenschutzgesetz grundsätzlich deren Löschung vor. Die Erforderlichkeit der Dauer der Datenspeicherung legt die datenverarbeitende Stelle in allgemeinen Regelungen über die Aufbewahrung von Daten fest. In einer solchen **Aktenordnung** müssen also Regelungen darüber enthalten sein,

- **welche Daten** gespeichert werden sollen,

- **für welche Dauer** die Speicherung beabsichtigt ist,

- **zu welchem Zweck** die Speicherung erfolgt.

Diese Anforderungen gelten auch, für **Personalräte,** wenn sie als selbständige datenverarbeitende Stelle Daten der von ihnen betreuten Mitarbeiter speichern.



Der Erlaß einer entsprechenden Aktenordnung wird zu einer deutlichen Reduzierung der bei den Personalräten gespeicherten Personaldaten führen und dadurch auch zur **Vereinfachung** der gesamten Schriftgutverwaltung beitragen. Für die Betroffenen ist die Datenverarbeitung der Personalräte transparenter geworden.

5. Datenschutz bei Gerichten

5.1 MEGA

Obwohl keine ausdrückliche Rechtsvorschrift die automatisierte Sammlung und Verarbeitung personenbezogener Daten in Gerichtsverfahren regelt, ist das „Mehrländerverfahren" (MEGA) in der derzeit geplanten Form datenschutzrechtlich nicht zu beanstanden. Der Bundesgesetzgeber bleibt jedoch aufgefordert, endlich die Prozeßordnungen unter datenschutzrechtlichen Gesichtspunkten zu ergänzen.

Im 17. Tätigkeitsbericht (Tz. 4.4.2) wurde über die verschiedenen Automationsvorhaben der Justiz berichtet. Aufgrund der Erfahrungen mit der „Geschäftsstellenautomation der Staatsanwaltschaften" (vgl. Tz. 4.4.1 dieses Berichts) haben wir den Justizminister auf die Rechtsprobleme aufmerksam gemacht, die sich aufgrund der in den Prozeßordnungen fehlenden, bereichsspezifischen, präzisen Regelungen für die Verarbeitung personenbezogener Daten bei neuen Automationsvorhaben ergeben können. Dies hat zur frühzeitigen Vorlage erster Konzepte für das Verfahren **MEGA** und zur Bitte um dessen datenschutzrechtliche Begutachtung geführt.

Wir konnten feststellen, daß hier grundlegend anders vorgegangen wurde als beim GAST-System. Geplant ist eine Lösung, die für jedes Gericht einen eigenen Abteilungsrechner vorsieht, eine

Stichwort MEGA

„MEGA" ist die Abkürzung für „Mehrländer-Gerichts-Anwendung". So nennen die Bundesländer Brandenburg, Schleswig-Holstein und Thüringen ihr gemeinsam neu entwickeltes EDV-Programm für die Gerichte. Es soll erstmalig in der deutschen Justiz die vollständige Einbindung der Arbeitsplätze von Richtern und Rechtspflegern, Aktenverwaltung und Schreibdienst verwirklichen. Vor allem für die vielen kleinen Gerichte erhofft man sich damit eine deutliche Verbesserung der Arbeitsbedingungen u.a. durch den Wegfall von Transportwegen, weniger Zeitaufwand für Absprachen, schnellere Erledigung von Schreibarbeiten. Den Richtern sollen bessere Informationsmöglichkeiten (z.B. durch die Abfrage von jurististen Datenbanken) die Entscheidungsfindung erleichtern.

Vernetzung mit anderen Rechnern findet nicht statt. Ein **landesweiter Zugriff** auf Gerichtsdaten ist somit **ausgeschlossen**.

Auch innerhalb der einzelnen Gerichte soll die **Abschottung** der verschiedenen **Abteilungen** so erhalten bleiben, wie sie bereits jetzt in der konventionellen Datenverarbeitung besteht. Es soll keine Zentralkartei angelegt werden, anhand der auf einen Blick alle eine bestimmte Person betreffenden Vorgänge erkennbar wären. Gespeichert werden sollen ausschließlich die zum Auffinden eines Vorganges erforderlichen personenbezogenen Daten: Vor- und Zuname, Anschrift, Geburtsname, Geburtsdatum, Geburtsort, Sterbedatum, Staatsangehörigkeit, Familienstand, Name der Mutter.

Aus den einzelnen Prozeßordnungen ergeben sich indirekt Hinweise auf die Daten, die der Gesetzgeber für unabdingbar hält, um eine sachdienliche Bearbeitung überhaupt durchführen zu können. Für MEGA reichen die vorhandenen gesetzlichen Grundlagen aus, wenn die Datenverarbeitung nicht über das Maß hinausgeht, das nach diesen Vorschriften für die Bearbeitung der jeweiligen Verfahren unverzichtbar ist.

Wir haben den Justizminister allerdings auf folgende noch offenen Einzelfragen hingewiesen:

- Durch das System soll der Bearbeiter auf evtl. notwendige Mitteilungen nach den Vorschriften der „**Mitteilungen in Zivilsachen**“ und „**Mitteilungen in Strafsachen**“ hingewiesen werden. Bei beiden Vorschriften handelt es sich nicht um Gesetze, sondern nur um Verwaltungsvorschriften, für die der Übergangsbonus abgelaufen ist. Diese Funktion sollte deshalb bis zur Verabschiedung eines Justizmitteilungsgesetzes außer Kraft bleiben.

- Das System soll eine „**Liste der Freizeitarreste**“ enthalten. Eine solche Erfassung ist im Gesetz nicht vorgesehen. Derartige Daten müssen nach Verbüßung vollständig gelöscht werden, damit hier nicht ein zweites Strafregister entsteht.

- Besonders klärungsbedürftig erscheint uns die geplante Einrichtung „**persönlicher Textfelder**“. Dadurch soll der Sachbearbeiter die Berechtigung erhalten, eigene Texte im System zu entwerfen, zu bearbeiten und zu speichern. Hier besteht die Gefahr, daß entscheidungsrelevante Informationen außerhalb der Prozeßakten abgelegt werden. Man sollte auf dieses Feld gänzlich verzichten, zumindest aber durch Dienstanweisung regeln, welche Informationen dort erfaßt werden dürfen, wie der Grundsatz der Aktenvollständigkeit gewahrt wird und wie die Einhaltung dieser Regelungen überwacht werden kann.

- Letztlich muß MEGA den Vorschriften des Landesdatenschutzgesetzes hinsichtlich des Schutzes der Mitarbeiterdaten genügen; automatisierte Verfahren dürfen nicht zu Zwecken der **Verhaltens- und Leistungskontrolle** genutzt werden.

Auch zu Fragen der **Sicherheit und Ordnungsmäßigkeit** des Verfahrens war auf eine Reihe von kritischen Punkten aufmerksam zu machen:

- Die **unbefugte** Speicherung und Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten ist zu **verhindern**. Dabei ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

- Es ist zu **gewährleisten**, daß **überprüft** und **festgestellt** werden kann, wer welche Daten eingegeben und aus MEGA heraus an Dritte übermittelt hat.

- **Verändernde Zugriffe** auf Programme zur Systemsteuerung und freigegebene Anwendungen dürfen nur von ausdrücklich dazu bestimmten Personen erfolgen.

- Automatisierte Verfahren dürfen erst eingesetzt werden, nachdem sie von der datenverarbeitenden Stelle **freigegeben** worden sind.

- Die Arbeit der **Systemadministratoren** ist durch weisungsbefugte Mitarbeiter oder deren Beauftragte kontinuierlich zu überwachen.



Zusammenfassend läßt sich allerdings feststellen, daß zum gegenwärtigen Zeitpunkt keine Veranlassung besteht, gegen das beabsichtigte Verfahren MEGA so grundlegende Bedenken zu erheben, daß dem Justizminister von einer Weiterverfolgung des Projektes abzuraten gewesen wäre.

Was ist zu tun?
Der Justizminister sollte bei der Realisierung von MEGA unsere Verbesserungsvorschläge berücksichtigen.

5.2 Zweckbindung von Daten, die in Prozessen erhoben worden sind

Die Frage, ob Daten einer Partei in einem Zivilprozeß ohne weiteres und ohne deren Einverständnis in anderen Verfahren verwandt werden dürfen, bedarf dringend der gesetzlichen Klärung.

Fast täglich kommt es vor, daß Menschen in der Ausnahmesituation einer Gerichtsverhandlung bereitwillig sehr intime Angaben machen oder sie sogar aufgrund einer Aussageverpflichtung machen müssen. Nicht selten

werden diese Daten ohne ihr Einverständnis in **anderen Prozeßarten** und in einem völlig anderen Zusammenhang weiter verwendet. So mußte ein Petent erleben, daß ihm Angaben über seine Vermögensverhältnisse, die er im Rahmen eines Ehescheidungsverfahrens gemacht hatte, plötzlich in einem anderen Zivilverfahren entgegengehalten wurden, weil in beiden Prozessen **zufällig derselbe Richter** zuständig war.

Ob personenbezogene Daten, die in einem bestimmten Verfahren freiwillig von Betroffenen preisgegeben werden, ohne weiteres und insbesondere ohne deren Einverständnis in anderen Verfahren verwandt werden dürfen, ist gesetzlich nicht geregelt. Leider besteht derzeitig die Praxis der Gerichte, hier einen Datenaustausch nach Zweckmäßigkeitsgesichtspunkten zu praktizieren, sofern dem nicht besondere Berufs- oder Amtsgeheimnisse (z.B. Steuergeheimnis) entgegenstehen. Dies ist nach unserer Ansicht datenschutzrechtlich bedenklich. Mangels einer spezialgesetzlichen Regelung kommen hier zwar die Vorschriften des Landesdatenschutzgesetzes über die **Zweckbindung** zum Tragen. Demnach dürfen Angaben, die ein Betroffener freiwillig für einen bestimmten Zweck macht, nicht ohne sein Einverständnis für andere Zwecke verwandt werden. Die Streitfrage, ob als Zweck, für den die Daten zur Verfügung gestellt werden, nur der eine Prozeß anzusehen ist oder ob darunter generell „Justizzwecke" zu verstehen sind, muß zugunsten der Betroffenen entschieden werden. Der Gesetzgeber ist deshalb aufgerufen, hier im Interesse der Betroffenen wie auch der Richter für Klarheit zu sorgen.



Was ist zu tun?

Der Justizminister sollte darauf drängen, daß die Prozeßordnungen an die Anforderungen des Volkszählungsurteils angepaßt werden.

6. Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung

6.1 Erfahrungen mit der neuen Datenschutzverordnung

„Von Praktikern überwiegend akzeptiert, von Entscheidungsträgern häufig ignoriert", auf diese kurze Formel lassen sich die Erfahrungen mit der neuen Datenschutzverordnung bringen. Trotzdem haben die neuen Regelungen eine Trendwende eingeleitet.

Da man mit der Festschreibung von Grundsätzen für eine sichere und ordnungsgemäße Datenverarbeitung in Form einer Rechtsverordnung datenschutzrechtliches Neuland betreten hat (vgl. 16. TB, Tz. 6.2), haben wir mit großer Spannung verfolgt, welche **Akzeptanz** die Datenschutzverordnung in der Praxis erfahren würde. Die ersten Reaktionen der „Verwaltungsdatenverarbeiter" während der zahlreichen Schulungsveranstaltungen in der DATENSCHUTZAKADEMIE, bei einzelnen Behörden und in unserem Haus waren bei weitem positiver, als wir zunächst vermutet hatten. Bezeichnend ist jedoch eine von den Praktikern häufig gebrauchte Formulierung: „Für mich ist die Angelegenheit jetzt klar. Wer überzeugt aber meinen Amtsleiter?"

Das sich dahinter verbergende Grundproblem ist auch in den Beratungsgesprächen und datenschutzrechtlichen Prüfungen des letzten Jahres deutlich zutage getreten: Bei denjenigen Mitarbeitern, die für die Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung unmittelbar zuständig sind, setzt sich immer mehr die Erkenntnis durch, daß die in der Verordnung geregelten Sicherheitsaspekte der Datenverarbeitung genauso wichtig sind wie die Fragen der Rechtmäßigkeit und Richtigkeit der Ergebnisse. Insoweit ist eine **positive Trendwende** gegenüber der früher vorherrschenden Einstellung der „Macher" unverkennbar.

Im gleichen Maße tut sich jedoch ein Graben zu denjenigen auf, die die erforderlichen personellen, organisatorischen und sachlichen Voraussetzungen zu schaffen haben, nämlich die **Entscheidungsträger** in den Behördenspitzen und in den sonstigen Leitungsgremien (Kommunalparlamente, übergeordnete Behörden, Aufsichtsgremien usw.). Vielen von ihnen ist das Hemd der **kurzfristigen Rationalisierungseffekte** noch immer näher als die Jacke einer auf Dauer funktionierenden, **professionellen Datenverarbeitung**. Diese unterschiedlichen Wirkungen der Datenschutzverordnung lassen sich an folgendem deutlich machen:

Das Landesdatenschutzgesetz und die Datenschutzverordnung enthalten zu dem Thema „Sicherheit und Ordnungsmäßigkeit" Bestimmungen, die sich in nur **15 Grundregeln** zusammenfassen lassen.

- ❑ Bereits in der Planungsphase sind Sicherheitskonzepte und Risikoanalysen zu erstellen (vgl. hierzu Tz. 6.2).

- ❑ Es ist frühzeitig festzulegen, in welchem Umfang Verfahrensabläufe zur Durchführung von Kontrollen zu dokumentieren sind.

- ❑ Die tatsächlich eingesetzte Hard- und Software ist vollständig zu registrieren.

- ❑ Die Datenstrukturen sind in Dateibeschreibungen darzustellen.

- ❑ Alle automatisierten Verfahren sind in Form von Aufgaben- und Verfahrensbeschreibungen zu dokumentieren.

- ❑ Unbefugten ist der Zugang zu bzw. die Benutzung von Datenverarbeitungsgeräten zu verwehren.

- ❑ Unbefugte Speicherungen sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten ist zu verhindern. Dabei ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

- ❑ Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in das Datenverarbeitungssystem eingegeben worden sind.

- ❑ Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an wen welche Daten übermittelt worden sind.

- ❑ Es ist zu verhindern, daß bei der Übertragung von Daten sowie während der Lagerung und des Transports von Datenträgern Daten unbefugt gelesen, kopiert, verändert, gelöscht oder entwendet werden können. Bei mobilen Datenverarbeitungsgeräten (z.B. Laptops) sind Datenbestände zu verschlüsseln.

- ❑ Es ist sicherzustellen, daß verändernde Zugriffe auf Programme zur Systemsteuerung und auf freigegebene Anwendungsprogramme nur durch dazu ausdrücklich bestimmte Personen erfolgen können.

- ❑ Vor Aufnahme der Verarbeitung sind die Programme und Verfahren zu testen, Art, Umfang und Ergebnis der Tests sind zu protokollieren.

- ❑ Automatisierte Verfahren dürfen erst eingesetzt werden, nachdem die datenverarbeitende Stelle mit der Freigabe die Verantwortung für die Ordnungsmäßigkeit des Verfahrens übernommen hat; die Freigabe ist zu protokollieren.

- ❑ Die ordnungsgemäße Anwendung der Datenverarbeitungsverfahren und insbesondere die Arbeit der Systemadministration ist durch weisungsbefugte Mitarbeiter oder deren Beauftragte kontinuierlich zu überwachen.

- ❑ Für den Fall, daß externe Dienstleister eingesetzt werden, sind diese sorgfältig auszuwählen, ihnen sind detaillierte schriftliche Weisungen zu erteilen, und es ist zu gewährleisten, daß die Daten nur im Rahmen dieser Weisungen verarbeitet. werden können.

Fragt man einen **Praktiker**, ob eine oder mehrere dieser Grundregeln entbehrlich, praxisfremd oder gar im Ergebnis falsch seien, wird man wie wir in unseren Beratungsgesprächen in der Regel die Antwort erhalten, sie seien „schon in Ordnung", letztlich werde durch sie eine **vernünftige Richtschnur** festgelegt.

Konfrontierten wir jedoch die **Entscheidungsträger** mit den logischen Konsequenzen aus der Beachtung der von ihren eigenen Mitarbeitern gutgeheißenen Grundsätze ordnungsgemäßer Datenverarbeitung, wurde uns häufig ein ganzer Strauß von (angeblich) gerade in diesem besonderen Fall unüberwindbaren **Sachzwängen entgegengehalten**:

- Man sei ja für eine ausreichende Planungsphase und für Sicherheitskonzepte. Aus Zeitgründen habe man aber bereits jetzt mit der Verarbeitung von Echtdaten beginnen müssen. Die Sicherheitslücken würden zu einem späteren Zeitpunkt geschlossen (vgl. Tz. 6.2).

- Für die effektive Verwaltung der Hardware und die Dokumentation der Verfahren fehle zur Zeit das Personal. Sobald jemand freigesetzt werden könne, werde man alles nachholen.

- Differenzierte Zugangs-, Benutzungs- und Zugriffsregelungen stünden einem im Augenblick unabdingbaren flexiblen Personaleinsatz entgegen.

- Bezüglich der Protokollierung von Verarbeitungsabläufen müsse man Rücksicht auf die Akzeptanz der Mitarbeiter und auf die Personalräte nehmen.

- Die Kontrolle der Systemadministratoren und der externen Dienstleister sei wegen der hierzu erforderlichen Fachkenntnisse sehr kostenaufwendig. Wichtig sei, daß man Vertrauen habe.

- Bezüglich der Intensität der Tests als Voraussetzung für die Freigabe von automatisierten Verfahren müsse doch „die Kirche im Dorf bleiben". Schließlich passierten ja auch bei der konventionellen Datenverarbeitung Fehler (vgl. Tz. 6.3).

- Im übrigen koste alles Geld, das nun einmal wegen der „im Augenblick angespannten Finanzlage" definitiv nicht zur Verfügung stehe.

Das zeigt, daß bezüglich der notwendigen Maßnahmen zur Umsetzung der Regelungen des Landesdatenschutzgesetzes und der Datenschutzverordnung in vielen Fällen auf der „Arbeitsebene" einfacher ein Konsens zu erzielen ist als auf der **Managementebene**. Dies sollte dem Gesetz-



geber, den Aufsichtsbehörden und den Behördenleitungen zu denken geben. In dem Maße, wie die Komplexität der Automatisierung steigt, werden derartige **Fehlentscheidungen** der Verantwortlichen an rechtlicher und auch an **wirtschaftlicher Tragweite** gewinnen. Hierzu gibt es bereits erste Beispiele (vgl. Tz. 6.2).

Was ist zu tun?
Die Leitungsebene der Verwaltungen muß die Datenschutzverordnung konsequent umsetzen.

6.2 Sicherheitskonzepte ohne Wenn und Aber

Jährlich werden vom Land, den Kommunen und den sonstigen öffentlichen Stellen mehrstellige Millionenbeträge in die Beschaffung neuer Computer und Programme investiert. Wegen fehlender Sicherheitskonzepte geht man bei der Benutzung der neuen Systeme vielfach unvertretbare Risiken ein. Fast scheint es, als wollte man mit Absicht erst aus Fehlern lernen.

Wir könnten uns die Sache einfach machen: In der Datenschutzverordnung ist verbindlich vorgeschrieben, daß bereits in der Planungsphase automatisierter Verfahren Sicherheitskonzepte zu entwickeln sind (vgl. auch Tz. 6.1). Stellen wir bei Prüfungen fest, daß dies nicht geschehen ist, könnten wir eine Beanstandung aussprechen und die betreffende Behörde auf die durch Planungsmängel entstandenen Sicherheitslücken hinweisen. Im günstigsten Falle würde die Behörde nachbessern, im ungünstigsten Fall blieben die Lücken bestehen.

Es dürfte allen einsichtig sein, daß dies auf Dauer kein gangbarer Weg ist. Wie können wir aber erreichen, daß im Hinblick auf die derzeit zu beobachtende Ausweitung der automatisierten Datenverarbeitung im Lande die Aspekte der Sicherheit, Revisionsfähigkeit und Ordnungsmäßigkeit nicht auf der Strecke bleiben? Führen wir uns vor Augen: Im Augenblick werden jährlich **mehrstellige Millionenbeträge** vom Land, von den Kommunen und den sonstigen öffentlichen Stellen in neue Projekte der Informations- und Kommunikationstechnik investiert. Das Spektrum ist so breit und vielschichtig, daß offensichtlich niemand im Land einen genauen Überblick hat. Uns sind z.B. folgende in der Planung bzw. Realisierung befindlichen Großprojekte bekannt:

- COMPAS - Bürokommunikation und Arbeitsplatzautomation im Bereich der Landespolizei (vgl. Tz.4.2.8),
- MEGA - Geschäftsstellenautomation der Gerichte (vgl. Tz.5.1),
- MOSAIK - Neugestaltung des Computereinsatzes in der Kommunal-

verwaltung (vgl. Tz.6.7.3),

- FIS - Finanzinformationssystem der Kommunen (vgl. Tz.6.7.3),
- ALK - Automation des Liegenschaftskatasters,
- FISKUS - Verbundentwicklung der IT-gestützten Besteuerungsverfahren,
- IKOTECH II - zweite Ausbaustufe des Bürokommunikationssystems der Landesregierung,
- INVEKOS - automatisierte Verfahren zur Struktur- und Einkommensförderung im Bereich der Landwirtschaft,
- Personalverwaltungs- und -managementsystem für den kommunalen Bereich,
- Personalverwaltungs- und -managementsystem für den Bereich des Landes,
- Patienteninformationssysteme in öffentlichen Krankenhäusern,
- verschiedene Umweltinformationssysteme.

Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit, zumal praktisch in allen Verwaltungszweigen weitere Projekte in den Schubladen liegen.

Soweit die Projekte in der IT-Kommission des Landes oder in der Automationskommission der kommunalen Landesverbände beraten worden sind (in beiden Gremien sind wir mit beratender Stimme vertreten), mußten wir feststellen, daß in **keinem einzigen Fall** bereits in der **Planungsphase ein Sicherheitskonzept** bestanden hat, das diesen Namen wirklich verdiente. Das Thema „Datenschutz und Datensicherheit“ wurde in den Beschlußvorlagen in der Regel auf knapp einer Seite mit dem Hinweis auf die Wichtigkeit und die Notwendigkeit, insoweit noch ergänzende Untersuchungen anzustellen, abgetan. Gleichwohl ist von diesen Steuerungsgremien bisher kein Automationsvorhaben gestoppt worden. Uns blieb in den Sitzungen nur die Möglichkeit, mahnend darauf hinzuweisen, daß nicht nur gegen datenschutzrechtliche Vorschriften verstoßen werde, sondern auch gegen die eigenen Richtlinien der Gremien (vgl. 15. TB, Tz. 6.3.3).

Dabei handelt es sich keineswegs nur um Formalien. Wie die unter Tz. 6.7 dargestellten Prüfungsergebnisse zeigen, bedingen die zur Zeit auch in kleinen Organisationseinheiten installierten Hochleistungs-IT-Systeme eine professionelle Administration, soll sich ihr Nutzen nicht in **unbeherrschbare Risiken** verkehren. Wenn aber weder der zum Systembetreuer „gemachte" Mitarbeiter noch sein Vorgesetzter geschweige denn der Behördenleiter überhaupt wissen, welche Risiken die von ihnen praktizierte Form der automatisierten Datenverarbeitung birgt, muß man sich nicht wundern, wenn bei Prüfungen Sicherheitsmängel gleich dutzendweise festgestellt werden. Deren nachträgliche Beseitigung kostet in der Regel erheblich mehr Geld, als wenn man von Anfang an die Vorschriften beachtet hätte. So nimmt es nicht wunder, daß sich uns bezüglich dieser Problematik ein Mitstreiter angeschlossen hat. Der **Landesrechnungshof** hat in einem Prüfbericht gegenüber dem Finanzminister die Forderung erhoben, alle Haushaltsmittel für Investitionen in IT-Projekte zunächst mit einem Sperrvermerk zu versehen. Die Freigabe der Mittel sollte vom Vorliegen eines geprüften Sicherheitskonzeptes abhängig gemacht werden. Dem können wir uns nur anschließen.



Was ist zu tun?
Bei der Planung neuer Datenverarbeitungsverfahren ist die Erarbeitung eines Sicherheitskonzeptes von Anfang an unverzichtbar.

6.3 Pilotprojekte - alter Wein in neuen Schläuchen

Bei der Entwicklung neuer automatisierter Verfahren dürfen die Bürger nicht dadurch zu „Versuchskaninchen" werden, daß man ihre Daten in unzulänglich ausgereiften und schlecht abgesicherten Pilotprojekten zu Testzwecken benutzt.

Wenn ein Unternehmen einen neuen Auto- oder Flugzeugtyp entwickelt, durchläuft dieser als Prototyp und als Vorserie eine große Anzahl von **Praxistests**. Dabei wird unter möglichst realitätsnahen Bedingungen geprüft, ob die aufgrund theoretischer Modelle entwickelte Konstruktion tatsächlich die Anforderungen erfüllt, die man an sie stellt. Je größer die Sicherheitsrisiken sind, um so intensiver sind diese Tests. Allein schon aus Haftungsgründen käme kein Hersteller auf die Idee, diese Testphase mit den bzw. an den Kunden selbst durchzuführen.

Im Bereich der Entwicklung von automatisierten Verfahren zeichnet die Realität ein deutlich anderes Bild. Nicht nur, aber gerade in der öffentlichen Verwaltung versucht man, den Zeitrahmen und damit die Kosten für die Konzeptions- und Testphase weitestgehend zu reduzieren. Dabei treten altbekannte und kritisierte Verfahrensweisen nicht selten in einem neuen Gewand auf. Haben wir uns in früheren Jahren gegen ausschließliche Tests durch die Programmierer selbst und gegen Tests mit Echtdaten

gewandt (vgl. 13. TB, Tz. 6.3), so müssen wir heute Bedenken erheben gegen sogenannte **Pilotprojekte**. Obwohl die Begriffe „Pilotprojekt", „Pilotphase", „Pilotkunde" usw. zunächst ganz unverfänglich erscheinen, verbirgt sich hinter ihnen häufig nichts anderes als die Absicht, ein automatisiertes Verfahren bereits zu einem Zeitpunkt in der Praxis einzusetzen, zu dem noch nicht alle materiell-rechtlichen und sicherheitstechnischen Voraussetzungen geschaffen worden sind. In vielen Fällen ist zum Zeitpunkt der „Pilotierung" noch nicht einmal die Konzeptionsphase abgeschlossen.

Wortreich wird diese Verfahrensweise als besonders „modern", weil effektiv, bezeichnet. Die „konservative" Methode der Softwaretests habe doch gezeigt, daß man mit ihr auch nicht alle Fehler hat aufspüren können. Hier zeigt sich die ungute Dialektik: Unzulänglichkeiten der einen Methode sollen die Schwächen einer anderen rechtfertigen. Wenn mit „unfertigen" Hardware- und Softwarekomponenten „echte" personenbezogene Daten verarbeitet werden, ist das Risiko, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden, unvertretbar hoch. Andernfalls bräuchte man die Verfahren ja nicht weiterzuentwickeln, sie wären ja bereits „O.K."!



Pilotprojekte sind deshalb datenschutzrechtlich nur zu akzeptieren, wenn die betreffenden automatisierten Verfahren konzeptionell und verfahrenstechnisch so weit gediehen sind, daß die im Landesdatenschutzgesetz und in der Datenschutzverordnung vorgegebenen Rahmenbedingungen erfüllt sind. Dies haben die verantwortlichen datenverarbeitenden Stellen durch die Einsatzfreigabe für die „Pilotierung" zu bestätigen.

Was ist zu tun?
Bereits in der Pilotphase muß das Datenschutzrecht in vollem Umfang eingehalten werden.

6.4 Computerdiebstahl - ein neues Phänomen

Werden PC gestohlen, geschieht dies in der Regel wegen des Wertes der Hardware. Man kann aber nicht sicher sein, daß der Dieb nicht auch mit den Datenbeständen Unheil anrichtet. Die Technik bietet hier die wünschenswerte Sicherheit durch Verschlüsselung.

Wird eine Akte gestohlen, dann bestimmt nicht wegen ihres Papierwertes, sondern, um andere zu kompromittieren, Beweismittel verschwinden zu lassen oder um die Tätigkeit der Behörde zu erschweren oder unmöglich zu machen. Im Zeichen der Computerisierung der Verwaltung werden viele papierene Akten durch die PC und die darin arbeitenden Festplatten ersetzt. Dabei entsteht ein überraschender Nebeneffekt: Der reine Papierwert von zwei Schränken voller Akten ist äußerst gering; wird die

gleiche Datenmenge in einem PC „gelagert", repräsentiert dieser einen Wert von ca. 5 000 DM. Da lohnt sich ein **Diebstahl des „Datenträgers"**, nicht der Akten.

So ist es nicht verwunderlich, daß uns auch im abgelaufenen Jahr mehr als ein **halbes Dutzend Diebstahlsfälle** bekanntgeworden sind. Praktisch alle Verwaltungsbereiche waren betroffen. Der Wert der gestohlenen Hardware schwankte pro Fall zwischen wenigen tausend und dreihunderttausend DM. Insbesondere wenn er durch eine Versicherung gedeckt war und die Geräte nicht zur Verarbeitung personenbezogener Daten benutzt werden, bereitete er den betroffenen Behörden kein größeres Kopfzerbrechen. Wer möchte aber in der Haut des Bürgermeisters stecken, aus dessen **Standesamt** der PC mitsamt aller **Registerdaten** (Geburten, Heiraten, Sterbefälle usw.) gestohlen wurde? Die Rekonstruktion der Dateien mit Hilfe der Sicherheitskopien war kein Problem. Wer konnte aber wissen, ob der Dieb es nur auf die Hardware abgesehen hatte oder ob er auch Kapital aus dem Inhalt des Personenstandsregisters schlagen wollte? An welcher Stelle und zu welchem Zeitpunkt würden Informationen über „sehr private" Familienverhältnisse prominenter Mitbürger auftauchen?

Nun kann man geltend machen, daß gegen einen Diebstahl mit Gewaltanwendung ohnehin „kein Kraut gewachsen" sei. Der Diebstahl des gesamten Computers sei nun einmal das nicht zu vermeidende Restrisiko. Dieser Standpunkt läßt jedoch die heute gerade durch die Technik verfügbaren Möglichkeiten außer acht (Sicherheit nicht nur wegen, sondern auch durch Technik). Es ist nämlich, wie bereits im 16. Tätigkeitsbericht (Tz. 6.5) in bezug auf tragbare Geräte beschrieben, aufgrund der heutigen internen Verarbeitungsgeschwindigkeiten kein Problem mehr, Datenbestände ohne Zeitverlust so wirksam zu **verschlüsseln**, daß jedem „normalem" Dieb die Lust daran vergeht, den Code zu knacken.

Als **wirksames Mittel** nicht gegen Computer-, aber gegen Datendiebstahl ist den Behörden also zu empfehlen:

- Möglichst alle Arbeitsplatzrechner vernetzen,
- die Datenbestände vernetzter Rechner zentral und besonders gut gesichert speichern,
- Datenbestände auf Einzelplatzrechnern verschlüsseln und
- die verwendeten Verschlüsselungssysteme zentral besonders gesichert verwahren.



Was ist zu tun?
Die Behörden sollten Vorkehrungen treffen, damit der Schaden für die Bürger bei Computerdiebstahl möglichst gering ist.

6.5 Viren nun auch in Dokumenten

Schon seit Jahren weiß man, daß Computerviren nicht nur auf Programmdateien beschränkt sein müssen. Trotzdem wurde die Fachwelt Mitte 1995 von einem Virus überrascht, der sich über Textdokumente ausgebreitet hat.

Die meisten Softwareprodukte für Textverarbeitung, Tabellenkalkulationen usw. erlauben, daß ihre Textdateien Steuerungsbefehle enthalten, die über die Tastatur eingegeben oder per Mausklick ausgeführt werden können. Der Benutzer kann mehrere Befehle zu einem „Makro" zusammenbauen, so daß richtige Programme entstehen. Viele Softwareprodukte stellen selbst eine große Menge von **Makrobefehlen** bereit, z.B. das Öffnen, Verändern oder Schließen von Dateien oder gar das Ausführen von Systemfunktionen. Auch das in der Verwaltung tausendfach eingesetzte Produkt „Word für Windows" besitzt eine umfangreiche Makrosprache und bietet die Möglichkeit, Makros automatisch auszuführen.

Stichwort Computerviren
Es sind sehr kleine Computerprogramme, die sich selbst vervielfältigen und so immer neue Systeme „infizieren". Sie können dort Schäden unterschiedlichster Art verursachen, z.B. gespeicherte Daten löschen oder verändern! Sie werden häufig von „Hackern" konstruiert, die Personen oder Unternehmen dadurch einen Schaden zufügen oder sich einfach nur einen Spaß machen wollen.

Word-Dokumente, die mit dem als ersten bekanntgewordenen **Makrovirus Winword-Concept** infiziert sind, enthalten Makrobefehle, die automatisch beim Laden der Datei von „Word" interpretiert und ausgeführt werden. Der Virus manipuliert die globalen Makroeinstellungen der Textverarbeitung und bewirkt, daß von nun an jede Datei beim Speichern ebenfalls infiziert wird.

Kurz nach dem ersten Makrovirus tauchten **weitere Viren** dieser Familie auf: „Winword-Nuclear" - pikanterweise durch ein Textdokument verbreitet, das vor dem ersten Virus warnte -, „Winword-Colors" und die DMV-Viren für Microsoft-Word und -Excel. Inzwischen soll es allein für Word zehn bis zwölf Makroviren geben. Während der erste Virus keine zerstörerischen Routinen enthält, ist der Winword-Nuclear-Virus so programmiert, daß die **Systemdateien** von MS-DOS jeweils **am 5. April vernichtet** werden.

Die heutige Situation ist wie folgt zu beschreiben:

- Die **Makroviren** können unabhängig vom Betriebssystem agieren und sich deswegen **systemübergreifend** ausbreiten.

- Für **jede Anwendung** mit einer hinreichend mächtigen Makrosprache

können solche Viren programmiert werden, also neben Textverarbeitungen auch für Tabellenkalkulationen oder Datenbanken.

- Text- und Tabellendokumente werden bedenkenlos **per Diskette** oder über ein **Netz ausgetauscht**, obwohl Antivirusprogramme keinen umfassenden Schutz bieten.

- Sieht die eingesetzte Software nicht vor, die Makrofunktion ständig abzustellen, läßt sich ein guter Schutz vor Makroviren lediglich mit Hilfe **ausgefeilter Zugriffsregelungen** erreichen, wie sie zusätzlich installierte Sicherheitswerkzeuge oder Betriebssysteme, die spezielle Sicherheitskriterien erfüllen (z.B. Windows NT), zur Verfügung stellen.

- Um zu gewährleisten, daß bei einer Weitergabe von Dokumenten im elektronischen Format keine Makroviren verteilt werden, kann man auf Formate ausweichen, bei denen keine Makros abgespeichert werden. Für formatierte Texte bietet sich das **Rich Text Format** (RTF) an, das von allen gängigen Textverarbeitungen verstanden wird. Für Tabellenkalkulationen kommt das standardisierte Data Interchange Format (DIF) in Frage.



Was ist zu tun?
Die datenverarbeitenden Stellen müssen bei ihren Datensicherheitsmaßnahmen auch der Bedrohung durch Viren in Dokumenten Rechnung tragen.

6.6 Was ist Original, was Kopie?

Änderungen und Ergänzungen schriftlicher Dokumente können in der Regel erkannt werden. Veränderungen an Computerdatenbeständen sind dagegen prinzipiell möglich, ohne Fingerabdrücke zu hinterlassen. Werden Daten ausschließlich in automatisierten Dateien gespeichert, sind Ausdrucke stets nur eine Kopie, so daß besondere Sicherheitsvorkehrungen zum Schutz des „Originals" notwendig sind.

Es mag sein, daß das papierlose Büro auf absehbare Zeit der unerfüllte Wunschtraum der Organisations- und Automationsreferenten bleiben wird. Trotzdem steht die „papierbasierte" Datenverarbeitung vor einem geradezu revolutionären Umbruch. Was im Bereich der Banken, Versicherungen, Bausparkassen und in anderen Bereichen der Wirtschaft bereits Realität ist, zeigt sich in der öffentlichen Verwaltung in ersten Ansätzen. Mehr und mehr Basisinformationen für Abrechnungen, Bescheide, Bewilligungen, Ablehnungen usw. sind nicht mehr in Akten bzw. auf Dokumenten schriftlich fixiert, sondern befinden sich in den

„virtuellen Akten“ der Rechnersysteme.

Bei der Erstellung eines **Kommunalabgabenbescheides** dürfte über kurz oder lang durchaus normal sein, daß ein Computerprogramm auf folgende Datenbestände zugreift:

- Grundstücksdatenbank (zur Ermittlung der Bezeichnung, der Größe, der Art der Nutzung und des Zuschnitts des Grundstücks),
- Grundstückseigentümerdatei (zur Ermittlung der Abgabepflichtigen),
- Melderegister (zur Ermittlung der aktuellen Anschrift der Abgabepflichtigen),
- Melderegister (zur Ermittlung der Anzahl der auf dem Grundstück wohnenden Personen),
- Energieverbrauchsdatei des Energieversorgungsunternehmens (zur Ermittlung des Wasserverbrauchs),
- Transportdatei des Entsorgungsunternehmens (zur Ermittlung der Art und des Gewichts des erzeugten Abfalls),
- Einheitswertdatenbank der Steuerverwaltung (zur Ermittlung des Einheitswertes und der Grundsteuerdaten),
- Buchhaltungsdatenbank (zur Ermittlung der bereits getätigten Vorauszahlungen),
- Datei der Bankverbindungen und Einzugsermächtigungen (zur Vorbereitung des Datenaustausches mit Banken und Sparkassen)
- usw. usw.

In wenigen **Millisekunden** werden alle Basiswerte eingelesen, die Abgabenmaßstäbe aus Tabellen, die im Computer abgelegt sind, hinzugefügt und ein Bescheid ausgedruckt, der **ohne Unterschrift automatisch kuvertiert und abgesandt** wird. Auf den Ausdruck einer „Verfügung“ für die Akten wird verzichtet, da sie auf Knopfdruck vermeintlich jederzeit an jedem Arbeitsplatz in der Verwaltung in beliebiger Anzahl neu erstellt werden kann.

Was aber, wenn die Basiswerte in der Zwischenzeit durch Eingabe- oder Programmfehler geändert worden sind? Wenn zu verschiedenen Zeiten unterschiedliche Ergebnisse errechnet/ausgedruckt worden sind, welches ist dann maßgeblich? Wer ist für den Inhalt verantwortlich, derjenige, der die Basiswerte, oder derjenige, der die Abgabenmaßstäbe erfaßt hat, oder etwa der Programmierer oder der Systembetreuer? Die Rechtsprechung

verlangt für die Wirksamkeit eines Verwaltungsaktes, daß er nicht ausschließlich automatisiert erstellt werden darf, sondern daß ein Mitarbeiter der Verwaltung letztlich die Entscheidung treffen muß. Welche Korrekturmöglichkeiten hat er aber, wenn der Verwaltungsakt das Resultat hochkomplexer Verarbeitungsabläufe ist?

Es ist daher nicht nur aus datenschutzrechtlichen Gründen dringend geboten, die Authentizität ausschließlich in automatisierten Dateien gespeicherten Datenbestände besonders wirksam zu sichern. Hierzu sind **neue organisatorische und technische Verfahrensweisen** zur Zugriffs-, Speicher- und Eingabekontrolle erforderlich.

Zuvor ist aber eindeutig festzulegen: Ist der Computerdatenbestand das Original, und sind die Ausdrucke nur eine Kopie oder umgekehrt? Bei einer Reihe neuentwickelter Verfahren war dies für uns selbst nach eingehenden Untersuchungen gemeinsam mit den Verfahrensentwicklern und Benutzern nicht immer eindeutig festzustellen (vgl. Tz. 4.2.8). Wir sehen deshalb die Gefahr, daß es in den nächsten Jahren verstärkt zu Situationen kommen wird, in denen die datenverarbeitenden Stellen intern nicht mehr feststellen oder nachweisen können, welche Daten zu welchen Zeitpunkten Gültigkeit hatten, und es nicht zu klären ist, welche **„Beweiskraft" Computerausdrucke** besitzen.

Was ist zu tun?

Die Behörden müssen klar festlegen, welcher Datenbestand der authentische ist: der in der Akte oder der im Computer gespeicherte. Ist letzteres der Fall, bedarf es spezifischer Sicherheitsmaßnahmen.

6.7 Ergebnisse von Prüfungskontrollen im Bereich der automatisierten Datenverarbeitung

6.7.1 Beanstandung akzeptiert ... (3. Auflage)

Die Ernsthaftigkeit der Bemühungen der Städte Kiel und Flensburg, datenschutzrechtliche und sicherheitstechnische Mängel abzustellen, ist nicht zu verkennen. Während man in Kiel nun offenbar endlich tätig werden möchte, bestehen in Flensburg nach wie vor Kapazitätsprobleme. Andere Behörden beseitigen die Defizite zügiger.

Die deutlichen Worte, mit denen wir im 17. Tätigkeitsbericht (Tz. 6.2.1) die Städte Kiel und Flensburg gemahnt haben, die im Rahmen von Prüfungen in den Jahren 1992 und 1993 beanstandeten datenschutzrechtlichen Mängel - wie von ihnen selbst versprochen - endlich zu beheben, haben ihre Wirkung nicht verfehlt. Dazu mag auch beigetragen haben, daß der Innenminister in den Beratungen des Tätigkeitsberichtes im Innen- und Rechtsausschuß von Abgeordneten gedrängt worden war, als

Kommunalaufsichtsbehörde tätig zu werden, falls die beiden datenverarbeitenden Stellen weiterhin so zögerlich agieren.

Auf Befragen hat uns die **Stadt Kiel** jedenfalls im November 1995 mitgeteilt, sie bedauere es sehr, daß ihre Aktivitäten sowohl in den parlamentarischen Gremien als auch in der Presse ausgesprochen negativ dargestellt worden seien. Sie müsse allerdings unsere Behauptung, hier liege eine offensichtliche Verzögerungstaktik vor, zurückweisen. Wir nehmen dies zur Kenntnis, stellen aber fest, daß z.B. eine bereits im Jahr 1992 angekündigte „Geschäftsanweisung für den Einsatz der technikunterstützten Informationsverarbeitung bei der Landeshauptstadt Kiel" erst am 23.06.1995 in Kraft getreten ist. Inhaltlich mag diese Geschäftsanweisung in einigen Punkten noch verbesserungsfähig sein. Gegenüber den im Jahr 1992 vorgefundenen Gegebenheiten wäre es jedoch ein großer Fortschritt, wenn diese Regelungen nunmehr in allen Bereichen der Stadtverwaltung strikt eingehalten werden. Außerdem hat die Stadt Kiel angekündigt, das Städtische Amt für Organisation und Verwaltungsreform beabsichtige, Anfang 1996 in einer Sonderaktion nochmals alle von uns seinerzeit angesprochenen Punkte aufzugreifen und sämtliche Ämter, Betriebe, Referate und Einrichtungen der Landeshauptstadt diesbezüglich zu überprüfen. Wir werden uns über die Ergebnisse dieser Aktion zu gegebener Zeit ein Bild machen.

Auch die **Stadt Flensburg** hat uns über den Sachstand unterrichtet. Dabei wird in dramatischer Weise deutlich, in welchem Umfang die Verwaltungen bereits in der Technik „verfangen" sind, ohne die notwendigen Sicherheitsaspekte gewährleisten zu können. Der Magistrat teilte uns mit: „Zu Ihrem Bericht ... haben wir am 27.04.1994 eine erste Stellungnahme abgegeben und verschiedene geplante Abhilfemaßnahmen aufgezeigt. Leider müssen wir zugestehen, daß es bei etlichen Punkten bis heute (27.11.1995) weitgehend bei Absichten und Planungen geblieben ist." Die Personalkapazität der Abteilung „Informationstechnik" sei nämlich durch die gewaltigen Probleme beim Einsatz eines neuen automatisierten **Finanzinformationssystems** und im Zusammenhang mit der Räumung des Rathauses zum Zweck der baulichen Sanierung vollständig gebunden worden. Beim **Finanzinformationssystem** müsse man das Verfahren ungewollt zur Unterstützung der Entwickler in der Datenzentrale im Echteinsatz testen. Dabei habe man leider feststellen müssen, daß Datenschutzaspekte bisher nur sehr begrenzt programmtechnisch abgedeckt seien. Hinzu komme, daß die Mitarbeiter der Stadtverwaltung ca. 30 Monate über diverse Räumlichkeiten im Stadtgebiet verteilt arbeiten müßten, da komme es entscheidend auf den Aufbau und das Funktionieren einer weitreichenden informationstechnischen Vernetzung an. Wörtlich kommt die Stadt Flensburg zu folgendem Fazit: „Realistisch betrachtet gehen wir davon aus, daß wir vor allem durch das erforderliche Aufarbeiten der Mängel im Finanzinformationssystem erst ab Ende des 1. Quartals 1996 den notwendigen Freiraum erhalten werden, um die auch aus unserer Sicht dringend erforderlichen Maßnahmen und Rege-

lungen zur besseren Gewährleistung des Datenschutzes endlich zu treffen. Diese Arbeiten erhalten dann erste Priorität und sollen im Laufe des kommenden Jahres umgesetzt werden."

Es ist zwar zu begrüßen, daß hier mit offenen Karten gespielt wird, auch ist die Ernsthaftigkeit der Bemühungen der Stadt anzuerkennen. Es bleibt aber die grundsätzliche Frage: Kann es verantwortet werden, daß neue datenverarbeitungstechnische Unzulänglichkeiten die Abarbeitung längst bekannter Mängel behindern? Anders formuliert: Sind die Datenverarbeitungsverantwortlichen in der Datenzentrale, in den Steuerungsgremien des Landes und der Kommunen und den Behördenleitungen sich wirklich sicher, daß derzeit bei der Einführung neuer Informationstechnik in der Kommunalverwaltung die Prioritäten richtig gesetzt werden? Zu den „Empfehlungen der Automationskommission der kommunalen Landesverbände zur Weiterentwicklung der technikgestützten Informationsverarbeitung in der Kommunalverwaltung Schleswig-Holsteins" (vgl. 15. TB, Tz. 6.3.4) und den „Leitaussagen zur Informationstechnik in der öffentlichen Verwaltung des Kooperationsausschusses ADV" (vgl. 16. TB, Tz. 6.1) bestehen jedenfalls erhebliche Divergenzen (vgl. hierzu auch Tz. 6.7.3).

Die Abarbeitung der datenschutzrechtlichen Defizite bei den anderen beiden im Jahr 1994 geprüften Behörden (vgl. 17. TB, Tzn. 6.2.3 u. 6.2.4) geht zügiger voran. Die **Stadt Norderstedt** konnte über eine Reihe in der Zwischenzeit erledigter Punkte berichten. Das **Umweltministerium** hat eine neue Dienstanweisung für den Umgang mit Datenverarbeitungsanlagen erarbeitet, die u.a. eine Aufgabenbeschreibung für die IT-Leitstelle sowie Regelungen für die Test- und Freigabeverfahren, die Protokollierung von verändernden Systemzugriffen, die Durchführung von Datensicherungen und die Verwendung von Datenträgern enthält.

Was ist zu tun?
Die Städte Kiel und Flensburg sollten unseren Beanstandungen nunmehr umgehend Rechnung tragen.

6.7.2 Verbesserungen beim Patientendatenschutz im Lübecker Klinikum - zentrale Probleme aber weiterhin ungelöst

Der Einsatz eines externen behördlichen Datenschutzbeauftragten hat offensichtlich zu einer Reihe von Maßnahmen zur Behebung von Mängeln in der allgemeinen Datensicherheit geführt. Über die Lösung von gravierenden Rechtsproblemen im Umgang mit Patientendaten wird bisher nur diskutiert, aber noch nichts Entscheidendes unternommen.

Der Umfang unserer Kritik an den unzulänglichen Sicherheitsmaßnahmen im Klinikum der Medizinischen Universität zu Lübeck (vgl. 17. TB,

Tz. 6.6.2) hat nicht nur in den parlamentarischen Beratungen des 17. Tätigkeitsberichts, sondern auch in der Öffentlichkeit ein starkes Echo ausgelöst. Daß wir in ein „datenschutzrechtliches Wespennest" gestochen haben, wie eine Zeitung schrieb, mag die nachstehende Aufzählung der wesentlichen Aktivitäten des aufgrund unserer Prüfung engagierten **externen behördlichen Datenschutzbeauftragten** verdeutlichen.

Bereits im ersten Jahr seiner Tätigkeit sah er sich z. B. zu folgenden, aus unserer Sicht längst überfälligen Maßnahmen veranlaßt:

- Unterrichtung der Mitarbeiter des Klinikums über das Datengeheimnis und ihre sonstigen datenschutzrechtlichen Pflichten,
- Durchführung einer Datenschutz-Situationsanalyse im gesamten Universitätsklinikum,
- Erarbeitung von Aufgabenbeschreibungen für die Datenschutzbeauftragten in den einzelnen Kliniken und Instituten,
- Schulung dieser Mitarbeiter,
- Herausgabe eines Datenschutzhandbuches,
- Beteiligung an der Entwicklung des Klinik-Kommunikations-Systems und anderer automatisierter Verfahren,
- Durchführung einer PC-Revision,
- Überprüfung spezieller weiterer datenschutzrechtlicher und sicherheitstechnischer Aspekte.

Eines der wesentlichen Rechtsprobleme konnte aber weder der Datenschutzbeauftragte noch die Ministerin für Wissenschaft, Forschung und Kultur zu einem befriedigenden Abschluß bringen. Es geht um die im 17. Tätigkeitsbericht (Tz. 6.6.2) dargestellte Verfahrensweise, daß Ärzte, die nicht an der Behandlung von Patienten beteiligt waren, deren **Krankenakten ohne Einverständnis zu Forschungszwecken** nutzten. Die Ministerin teilte uns dazu mit: „Hinsichtlich der grundsätzlichen Fragestellung zur datenschutzrechtlichen Einschränkung der Nutzung medizinischer Daten zu Forschungszwecken habe ich eine abschließende Klärung noch nicht herbeiführen können. Die Erörterungen mit den medizinischen Fakultäten der Universitäten sowie mit den Direktorien der beiden Universitätsklinika des Landes haben ergeben, daß eine stringente Anwendung der von Ihnen vertretenen Rechtsauffassung bedeuten würde, daß letztlich Tausende von Krankenakten nicht mehr zu Forschungszwecken zur Verfügung stehen würden."

[redacted]

Aus unserer Sicht ist diese Auskunft in mehrfacher Hinsicht **nicht akzeptabel**:

- Die Auffassung der Universitäten und der zuständigen Aufsichtsbehörden dokumentiert ein bedenkliches Verhältnis zum Patientengeheimnis und zum ärztlichen Standesrecht. Dies wird deutlich, wenn man sich den **Wortlaut der Berufsordnung** vor Augen führt: „Zum Zweck der 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." Eine klarer formulierte Rechtsnorm ist kaum vorstellbar. Ein Spielraum für eine mehr oder weniger „stringente Auslegung" besteht nicht.

- Es mag sein, daß bei Beachtung der Rechtslage eine bestimmte Anzahl von Patientenakten, die Behandlungen aus früheren Jahren dokumentieren, für Forschungszwecke nicht zur Verfügung stehen, weil die Datenbestände nicht anonymisiert werden können und eine Einwilligung der Patienten nicht zu erlangen ist. Die Behauptung, es handele sich um **Tausende von Akten**, erscheint schon deshalb **nicht stichhaltig**, weil nur ein kleiner Prozentsatz der vorhandenen Hunderttausenden von Akten überhaupt für retrospektive Forschungszwecke von Bedeutung ist und für Einzelfälle in der Regel mehrere vergleichbare Akten als Alternativen in Betracht kommen dürften.

- Wenn es aber von so essentieller Bedeutung wäre, daß grundsätzlich alle Patientenakten des Klinikums zu Forschungszwecken nutzbar sein müßten, dann ist nicht zu verstehen, daß nicht unmittelbar nach der Prüfungsmaßnahme im Herbst 1994 damit begonnen wurde, von den „neuen" Patienten entsprechende **Einwilligungserklärungen** zu erbitten. Immerhin werden in den Kliniken der Christian-Albrechts-Universität zu Kiel jährlich 45 000 und im Klinikum der Medizinischen Universität zu Lübeck jährlich 39 000 Patienten behandelt. Für rund 100 000 Patientenakten der Universitätsklinika im Lande hätte also die Nutzbarkeit für Forschungszwecke zwischenzeitlich rechtlich einwandfrei eröffnet werden können.

- Eine Klinik der Medizinischen Universität zu Lübeck übergibt bereits heute ausschließlich **anonymisierte Daten** an die Forschungs- und Statistikdateien im Institut für Medizinische Statistik und Dokumentation, ohne daß dies zu erkennbaren negativen Auswirkungen auf dem Gebiet der wissenschaftlichen Forschung geführt hat. Die Initiative zur Anonymisierung ist vom Klinikdirektor selbst ausgegangen! Es ist nicht nachzuvollziehen, warum in ein und demselben Klinikum mit so unterschiedlichen Maßstäben gemessen wird.

Zusammenfassend kann also festgestellt werden, daß die Abarbeitung der allgemeinen sicherheitstechnischen und organisatorischen Mängel bei der

personenbezogenen Datenverarbeitung im Klinikum offenbar mit der gebotenen Intensität in Angriff genommen worden ist, daß aber in bezug auf die Nutzung von personenbezogenen Daten für Forschungszwecke durch nichtbehandelnde Ärzte ein erhebliches **Handlungsdefizit** besteht. Diese Probleme sind in jedem Fall zu klären, bevor das geplante Klinik-Kommunikations-System in den „Echtbetrieb" überführt wird.

Was ist zu tun?
Das Wissenschaftsministerium sollte aus der eindeutigen Rechtslage für die Forschung mit Patientendaten die Konsequenzen ziehen.

6.7.3 Neues Finanzinformationssystem beanstandet

Bei Kontrollen in mehreren Kommunen haben wir gravierende Mängel des neuen Finanzinformationssystems beanstandet. Die Kommunen verlassen sich zu sehr auf den Softwarelieferanten Datenzentrale.

Nachdem in den vergangenen Jahren schwerpunktmäßig die Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung in großen Kommunen überprüft worden sind (vgl. Ausführungen zu den Prüfungen bei den Städten Kiel, Flensburg und Norderstedt im 16. TB, Tzn. 6.6.2 und 6.6.3; 17. TB, Tzn. 6.2.1 u. 6.2.3 sowie Tz. 6.7.1 dieses Berichts), haben wir im abgelaufenen Jahr damit begonnen, auch **mittlere** und **kleinere kommunale Organisationseinheiten** sicherheitstechnischen Kontrollen zu unterziehen. Prüfungen bei den Städten Kappeln und Glückstadt konnten abgeschlossen werden, Kontrollen in Ratzeburg, Eutin und anderen Städten befinden sich in der Auswertung.

Die **Prüfungsergebnisse weisen** in einer Beziehung eine **einheitliche Tendenz** auf: Die gravierendsten Sicherheitsmängel beruhen auf **Unzulänglichkeiten** in den **Konzepten** für die Ausgestaltung der informationstechnischen Systeme und die Verwaltungsverfahren. Nur selten werden konzeptionell vorgesehene Sicherheitskomponenten von den Benutzern der Systeme und Verfahren fahrlässig oder bewußt konterkariert. Diese Feststellung wird durch die nachfolgende Zusammenstellung von Sachverhalten, die wir in der Praxis vorgefunden haben, untermauert (auf die Zuordnung zu den einzelnen geprüften Stellen wird bewußt verzichtet, da es nicht darum geht, eine einzelne Verwaltung „an den Pranger" zu stellen, sondern einen Trend aufzuzeigen):

- Es **fehlen Datenverbeitungskonzepte**, aus denen sich für alle Beteiligten nachvollziehbar ergibt, wie und mit welchem Ziel die Verwaltungsabläufe automatisiert werden sollen (Soll-Regelung). Somit ist ein kritischer Abgleich zwischen Soll und Ist nicht möglich. Mängel werden nicht als solche erkannt, sondern als technikbedingte „Gege-

benheiten“ angesehen.

- Auf Arbeitsplatzrechnern wird **Software** vorgehalten, die gar **nicht** zur Ausführung der für das betreffende Gerät zugelassenen Anwendung **erforderlich** ist.

- Die **Benutzer** haben unkontrollierten **Zugriff auf Systemfunktionen** an Arbeitsplatz- oder Zentralrechnern.

- Zugriffsrechte auf der lokalen Ebene können aufgrund **fehlender Sicherheitssoftware** nicht anwenderbezogen erteilt werden.

- Versuche unbefugter Datenveränderungen und -löschungen sowie **Virenangriffe** können nicht abgewehrt werden.

- **Zentralrechner** können von den Mitarbeitern der Verwaltung aufgrund unzureichender Ausbildung nur eingeschränkt **administriert** werden.

- **Externe Systembetreuer** führen die Arbeiten **unkontrolliert** aus. In der Regel wird ihre Tätigkeit auch nicht protokolliert.

- **Diskettenlaufwerke** sind permanent für einen (in der Regel überflüssigen) Datenaustausch **geöffnet.**

- **Verfahrenstests** werden nur unzureichend durchgeführt und protokolliert; das gleiche gilt für Verfahrensfreigaben.

Diese Beispiele machen deutlich, daß die unter Tz. 6.1 dieses Berichts dargestellten Grundregeln weitgehend unbeachtet bleiben. So ist es nicht verwunderlich, daß wir bei unseren Prüfungen **Beanstandungen „im Dutzend“** aussprechen müssen.

Von besonderer Tragweite ist die Feststellung, daß derartige Sicherheitsmängel nicht nur auftreten, soweit kleinere Verwaltungen ihre automatisierte Datenverarbeitung selbst konzipieren. Auch wenn die **Datenzentrale** wie z.B. im Zusammenhang mit dem neuen **MOSAIK-Konzept** eingeschaltet ist, sind signifikante Mängel festzustellen. Kommunen, die derzeit mit Hilfe des **Finanzinformationssystems (FIS)** personenbezogene Daten im Echtbetrieb verarbeiten, müssen damit rechnen, daß bei einer eventuellen datenschutzrechtlichen Überprüfung aus **folgenden** Gründen **Beanstandungen** ausgesprochen werden:

- Das **Personenkontenkonzept** läßt keine hinreichend wirksamen Zugriffsbeschränkungen zu. Insbesondere im Hinblick auf das Melde-, das Steuer-, das Sozialgeheimnis und die Pflichten zur Verschwiegenheit über Personaldaten lassen sich Rechtsverstöße bei bestimmten Konstellationen nicht vermeiden.

- Einige der gewählten softwaretechnischen Lösungen lassen auf den Arbeitsplatzrechnern **keine** vollständige **Abschottung** gegen verändernde Zugriffe zu.

- Das Einspielen von neuer oder geänderter Software erfolgt ohne eine entsprechende Freigabeempfehlung durch die kommunalen Landesverbände. Eigene **Tests** können die datenverarbeitenden Stellen faktisch nicht durchführen, da sie in der Regel nicht über den genauen Inhalt der Änderungen informiert sind und nicht über entsprechende Testbestände verfügen.

- Die meisten datenverarbeitenden Stellen sind außerdem nicht in der Lage, die **Fernwartungsaktivitäten** wirksam zu überwachen. Im Ergebnis haben Behördenfremde die nahezu vollständige Verfügungsgewalt über Hardware, Software und Daten.

- Das MOSAIK-Konzept enthält keine hinreichenden, verbindlichen **Komponenten zur Datensicherheit**. Die datenverarbeitenden Stellen werden dadurch dazu verführt, keine ergänzenden eigenen Sicherheitskonzepte und Risikoanalysen zu entwickeln.

Gerade der letzte Punkt weist auf die Ursachen für diese Situation hin. Die kommunalen Kunden der Datenzentrale verlassen sich nur zu gern darauf, von ihr rechtliche und sicherheitstechnische „**Sorglospakete**“ zu erhalten. Immerhin sei es „ihre“ Datenzentrale, und die Produktentwicklung werde durch die Vertreter der kommunalen Landesverbände im Verwaltungsrat mit gesteuert, da könne man verlangen bzw. davon ausgehen, daß die Produkte dieses Hauses nicht nur rechtlich einwandfreie Ergebnisse liefern, sondern auch, daß die Hard- und Softwarekonzepte im vollen Umfang den datenschutzrechtlichen Anforderungen entsprechen. Die Datenzentrale weist dagegen auf die vertraglichen Realitäten hin: Sie sei nur Softwarehaus und Hardwarelieferant. Beratungsdienstleistungen seien nicht Gegenstand der Hard- und Softwarelieferung, sie müßten im Rahmen des Consultings gesondert berechnet werden. Die Verantwortung für den rechtmäßigen und sicheren Einsatz ihrer Produkte bei den Kunden könne sie nicht übernehmen. Gleichwohl hat sie Modifikationen an den betreffenden Verfahren angekündigt.

Das **Fazit** aus datenschutzrechtlicher Sicht lautet:

Solange die von der Datenzentrale zu erbringenden Leistungen und die ergänzenden eigenen „Obliegenheiten“ ihrer Kunden nicht für alle Verfahren eindeutig definiert werden, muß man auch weiterhin mit Rechts- und Sicherheitsproblemen rechnen. Es dürfte deshalb die Zeit reif sein für einen **„runden Tisch“**, der die Zusammenarbeit der kommunalen

[redacted]



Landesverbände, ihrer Automationskommission, deren Fachausschüsse, der Kommunalaufsichtsbehörden, der Rechnungsprüfungsbehörden, der Mitbestimmungsgremien und nicht zuletzt des Datenschutzbeauftragten auf eine neue, zukunftsorientierte Grundlage stellt.

Was ist zu tun?
Die datenschutzrechtlichen Mängel des neuen Finanzinformationssystems sollte die Datenzentrale so schnell wie möglich beseitigen.

6.7.4 Inanspruchnahme externer Dienstleister

Die Regelungen zum Sozialdatenschutz knüpfen die Zulässigkeit der Inanspruchnahme externer Dienstleister an strenge Bedingungen. Kostenüberlegungen verführen jedoch die Behörden häufig dazu, zu großzügige Maßstäbe anzulegen.

Eine Prüfung in der Versorgungsverwaltung zeigte auf, daß die Einschaltung externer Dienstleister in einem so sensiblen Bereich wie der Sozialdatenverarbeitung nur unter genauester Beachtung der gesetzlichen Rahmenbedingungen zu vertreten ist. Zwei Fallgestaltungen werden zur Zeit mit dem **Landesversorgungsamt** kontrovers diskutiert:

- Kann es akzeptiert werden, daß Altakten, die medizinische und Sozialdaten enthalten, einem privaten Unternehmen zur Vernichtung übergeben werden? Reicht es aus, wenn das Unternehmen sich vertraglich verpflichtet, die verschlossenen Aluminiumcontainer, in denen die Unterlagen bei der Behörde gesammelt werden, erst unmittelbar vor dem Schreddern zu öffnen, oder bedarf es der **Aufsicht** der Behörde beim **Transport** und bei der **Vernichtung**?

- Wir sind der Auffassung, daß sich aus den gesetzlichen Regelungen des Sozialgesetzbuches die Verpflichtung für den Sozialleistungsträger ergibt, auch in diesen Fällen die Verfügungsgewalt über zu vernichtende Sozialdaten zu behalten. Dies erscheint nur logisch, wenn man sich folgenden Ablauf vergegenwärtigt: Solange die Akten bearbeitet werden, gilt das strenge Sozialgeheimnis. Die Akten müssen stets unter Verschluß gelagert werden. Ist das Verfahren abgeschlossen, kommen sie bis zum Ablauf der Aufbewahrungsfrist in ein Archiv, zu dem nur bestimmte Mitarbeiter Zutritt haben. Steht die Vernichtung an, werden sie in einen verschlossenen Container geworfen, zu dem die Behörde selbst keinen Schlüssel hat. Haben sie aber das **Gebäude verlassen**, besitzt ein Unternehmen, das nicht Sozialleistungsträger ist, beides, den **Schlüssel und die Akten**.

- Im Rahmen der Prüfung der Anträge auf Versorgungsrenten usw. sind in der Regel umfangreiche **medizinische Untersuchungen** erforderlich. Zu diesem Zweck beschäftigt die Versorgungsverwaltung eigene Ärzte. Wenn aber spezielle fachärztliche Fragen zu klären sind oder wenn der eigene ärztliche Dienst überlastet ist, werden zusätzlich auch **externe Ärzte** eingeschaltet. Auf diese Weise gelangen Sozialdaten in den Besitz von Personen, die zwar einem speziellen Berufsgeheimnis unterliegen, die aber nicht zu den „Leistungsträgern" gehören. Die Frage lautet: In welchem Umfang und wie lange dürfen die Sozialdaten von diesen Personen gespeichert werden?

- Wir haben vom Landesversorgungsamt gefordert, daß in die vertraglichen Vereinbarungen mit den Ärzten hierüber **konkrete Festlegungen** aufgenommen werden. Aus datenschutzrechtlicher Sicht dürfen Antragsteller bei der Einschaltung externer Gutachter nicht schlechter gestellt sein, als wenn ein Mitarbeiter der zuständigen Behörde die Untersuchungen vornimmt. Es würde mithin dem Schutz des Sozialgeheimnisses dienen, wenn von den externen Ärzten verlangt würde, daß sie die Grundlagen und Einzelheiten der Begutachtung nur insoweit dokumentieren, wie sie dazu nach den standesrechtlichen Vorschriften verpflichtet sind. In den meisten Fällen dürfte es sich um einige wenige rein medizinische Daten handeln. Die Versorgungsverwaltung bezweifelt die rechtliche Möglichkeit, den Ärzten diesbezüglich Vorschriften zu machen.

Wir haben in dieser Angelegenheit das Sozialministerium eingeschaltet.

7. Neue Medien und Technologien

7.1 Multimedia

Multimedia wird die künftige Informationsgesellschaft prägen. Der Datenschutz muß von Anfang an gewährleistet sein.

„Multimedia" ist das Wort des Jahres 1995, wie die Gesellschaft für deutsche Sprache ermittelte. Es ist ein schillernder Inbegriff für die Reise in die **schöne, neue Medienwelt**. Eine exakte Definition fällt schwer: Multimedia ist mehr als nur eine Kombination unterschiedlicher Medientypen wie Text, Ton, Bild und Video. Dabei bildet Multimedia keine neue Technologie an sich, sondern führt lediglich basierend auf digitaler Technik bisher getrennte Technologien und Anwendungen zusammen. Der Benutzer kann typischerweise mit den Multimediasystemen interagieren.

Stichwort Multimedia
Durch bessere und schnellere Technik können Informationen „multimedial" vermittelt werden, d.h. wie beim Fernsehen werden gleichzeitig Augen und Ohren der Zuschauer angesprochen. Während zentrale Fernsehsender pro Kanal für alle dieselben Bilder ausstrahlen und die Zuschauer nur die Wahl zwischen den verschiedenen Programmem haben, werden die Benutzer bei der neuen Multimediatechnologie stärker einbezogen: Sie können in einen Dialog mit der jeweiligen Anwendung treten und individuell bestimmen, wann sie wie welche Informationen erhalten. Einkaufen oder Buchen einer Reise mit aktuellen Daten soll ebenso komfortabel von zu Hause aus möglich sein wie z.B. das gezielte Abrufen von Filmen oder Bildungsangeboten.

Einige Angebote laufen lokal auf dem Computer ab, z.B. Lexika oder Spiele auf CD-ROM. Andere Dienste sind nur über Telekommunikationsnetze verfügbar. Auch hier kommt der Computer auf dem Schreibtisch zum Einsatz. Der größere Markt wird jedoch im heimischen Wohnzimmer gesehen: Ein kleiner schwarzer Kasten, die sog. „Set-Top-Box", macht aus dem Fernseher eine Multimediamaschine. Die Box entschlüsselt digitale Signale und verwandelt sie in analoge Informationen für den Fernsehbildschirm. Die **Set-Top-Box** soll etwa 1 000 DM kosten und sich mit Fernseher, PC, Telefon und Stereoanlage verbinden lassen. Um auf die zahlreichen Multimedia-Anwendungen zugreifen zu können, muß der Benutzer nur eine mit Geld „gefüllte" Chipkarte, von der anfallende Gebühren abgebucht werden, in den Schlitz des Gerätes stecken. Die digitale Übertragungsform der Fernsehsignale schafft durch Kompression Platz für Hunderte von Kanälen; der erste Satellit für digitales Fernsehen Astra 1 E geht 1996 auf Sendung.

Die zur Zeit entwickelten Angebote sind auf alle Lebensbereiche ausgerichtet: Arbeit, Bildung, Freizeit, Handel. Sie erstrecken sich von Bildtelefon und Videokonferenzen über Lernprogramme, digitale Nachschla-

gewerke und Informationssysteme bis zu interaktiven Spielen, Video-On-Demand (Videofilme auf Anforderung), Homeshopping, Online-Diensten und Telemedizin - alles vom Fernsehsessel aus zugänglich. Das Fernsehen soll sich vom Massenmedium zum individualisierten Informations- und Unterhaltungsmedium mit „Rückkanal" wandeln.

Die Multimediatechnologie wird die künftige Informationsgesellschaft prägen und viele Bereiche unseres Lebens nachhaltig beeinflussen. Um so wichtiger ist es, bereits vor der Marktreife der Multimediaprodukte die Entwicklung aus Datenschutzsicht zu verfolgen und zu gestalten. Denn bei Inanspruchnahme vernetzter Anwendungen entstehen personenbezogene Daten, die nicht nur für Zwecke der Abrechnung nutzbar sind, sondern auch für die Programmanbieter unter Marketingaspekten interessant sein können. Es ließen sich detaillierte Informationen darüber speichern, wann welcher Nutzer welche Fernsehsendungen, Videos oder elektronische Zeitungsartikel abgerufen, welche Produkte er beim Homeshopping bestellt, wohin er Reisen elektronisch gebucht oder welche Abfragen er in Informationssystemen vorgenommen hat. Diese Daten könnten nach dem **Kommunikations- und Konsumverhalten** der Kunden ausgewertet werden und würden eine Ausforschung persönlicher Lebensgewohnheiten ermöglichen.

Der Zugang zu der neuen Technologie darf jedoch nicht mit dem Verlust der Privatsphäre verbunden sein. Daher ist eine **datensparsame Multimediatechnik** notwendig: Daten, die für einen Dienst nicht erforderlich sind, werden gar nicht erst erhoben; für die übrigen Daten gilt eine strenge Zweckbindung, die jede andere Verwendung ausschließt. Dabei soll der Datenschutz keinesfalls den technischen Fortschritt hemmen - im Gegenteil, er soll als „Feature" in die Technik eingebaut werden, was die Benutzerakzeptanz für die neuen Medien sicher erhöhen wird und von Herstellerfirmen als zusätzliches Marketinginstrument genutzt werden kann.

Wir stellen uns die technischen und organisatorischen Datenschutzmaßnahmen der Multimediatechnologie folgendermaßen vor:

- Die Systeme sind so **transparent** aufgebaut, daß jeder Benutzer durchschauen kann, wo welche Daten gespeichert sind und wie die Datensicherheit gewährleistet wird. Soweit möglich werden die Daten dezentral ausschließlich beim Benutzer selbst gespeichert, der allein entscheidet, wem er welche Daten zu welchen Zwecken zur Verfügung stellt.

- Die **Tarifstruktur** enthält Pauschalen, wodurch detaillierte Datensammlungen wegfallen können.

- Die Abrechnungsverfahren sehen **anonyme Zugänge** vor, die z.B. mit Hilfe von Guthaben-Chipkarten (Pre-Paid-Chipkarten) realisiert

werden. Durch Abbuchung von der im voraus bezahlten Karte bei Nutzung des Dienstes entfällt die Speicherung personenbezogener Daten.

- Die Datensicherheit der übertragenen Informationen wird z.B. durch wirksame **Verschlüsselung** gewährleistet. Dies ist bei Übermittlung anderer sensibler Daten, aber auch z.B. für eine sichere Abwicklung von Bankgeschäften von Bedeutung.

- Die **Kontrolle** der Einhaltung des Datenschutzes erfolgt durch unabhängige Stellen.

Wenn Datenschutz- und Sicherheitsmechanismen nicht bereits während der Konzeption und Entwicklung neuer Technik berücksichtigt werden, sind sie anschließend oft schwierig zu integrieren. Deswegen fordern wir eine **datenschutzgerechte Gestaltung** der Systeme **von Anfang an**. Dies gilt im besonderen Maße auch für Pilotprojekte, die bereits in einigen deutschen Städten laufen. Leider beinhaltet zur Zeit kein einziges Multimediapilotprojekt die Möglichkeit anonymer Dienstenutzungen, obwohl es aus unserer Sicht sinnvoll wäre, in einem solchen Rahmen verschiedene Konzepte anonymer Zugänge zu testen.

In **Schleswig-Holstein** gibt es bislang kein Pilotprojekt zu Multimedia, doch ist sich die Landesregierung offenbar der Wichtigkeit dieser neuen Technologie bewußt. Koordiniert von der Technologiestiftung Schleswig-Holstein hat sich nämlich im Berichtsjahr ein Arbeitskreis mit Vertretern aus verschiedenen Bereichen der Wirtschaft und der Verwaltung, einschließlich des Landesbeauftragten, zu dem Thema gebildet. Daraus hervorgegangen ist die **Studie „Telekommunikationstechnologien** - Bestandsaufnahme und Handlungsbedarf für Schleswig-Holstein". Sie soll dem Land als Grundlage für Aktionen im Bereich Multimedia dienen und den Handlungsbedarf sowie mögliche Handlungsansätze aufzeigen. Wir haben an der Studie mitgewirkt und werden für ggf. entstehende Projekte konkrete Vorschläge erarbeiten, wie sich Datenschutzmaßnahmen technisch integrieren lassen.

Was ist zu tun?
Bei der Entwicklung und Erprobung von Multimediavorhaben muß der Datenschutz der Kunden von Anfang an gewährleistet sein.

7.2 Liberalisierung des Telekommunikationsmarktes

Mit der dreiphasigen „Postreform" wird der Telekommunikationsbereich privatisiert. Es steht zu befürchten, daß die Datenschutzbestimmungen in den neuen Gesetzen aufgeweicht werden.

Die Postreform mündet Anfang 1998 in die Liberalisierung und Neugestaltung des Telekommunikationssektors: Nach dem Fall des Telekom-Monopols werden viele Unternehmen ihre Leistungen auf dem Telekommunikationsmarkt anbieten. In den zur Zeit vorbereiteten Gesetzen werden die Rechtsgrundlagen für den Telefondienst, aber auch für Multimedia und Online-Dienste geschaffen. Die rechtliche Ausgestaltung der letzten Stufe der Postreform soll ein neues **Telekommunikationsgesetz** (TKG) regeln, dessen derzeitiger Entwurf unter verschiedenen Gesichtspunkten zu kritisieren ist.

Da zukünftig durch weltweite Vernetzung, Multimedia und interaktive Dienste sehr viel mehr Telekommunikationsdienstleistungen als bisher in Anspruch genommen werden, kommt es darauf an, das Prinzip der Datenvermeidung bzw. Datenreduzierung gesetzlich abzusichern und auf einer engen Zweckbindung der erhobenen Daten zu bestehen. Sonst entsteht das Risiko, daß die Netzbetreiber und Diensteanbieter die „Datenspuren", die der Bürger bei der Nutzung der Leistungen hinterläßt, unkontrolliert auswerten können.

Darüber hinaus fordern wir, daß die Netzbetreiber und Dienstanbieter auch **anonyme Zugangs- und Nutzungsformen** für ihre Leistungen bereitstellen. Schließlich hängt die Akzeptanz der zukünftigen Informationsgesellschaft wesentlich von der Sicherung des Grundrechts auf **unbeobachtete Kommunikation** und von der Transparenz der technischen Verfahren ab.

Stichwort Postreform

Die Postreform bezeichnet eine Entwicklung in Deutschland vom vormals staatlichen Monopol zum freien Markt im Post- und Telekommunikationsbereich.
Sie wird in drei Stufen abgewickelt:
***Postreform I** (1989-1994):*
Die Deutsche Bundespost teilt sich in drei öffentlich-rechtliche Unternehmen. Die Telekom, das Unternehmen für den Bereich Telekommunikation, besitzt das Monopol bei der öffentlichen Netzinfrastruktur und beim Telefondienst. Davon ausgenommen sind Satelliten- und Mobilfunknetze, die von privaten Firmen aufgebaut und angeboten werden dürfen, zunächst jedoch ohne Sprachübermittlung.
***Postreform II** (1994-1997):*
Die entstandenen öffentlich-rechtlichen Unternehmen werden als Voraussetzung für die Einführung des Wettbewerbs in Aktiengesellschaften umgewandelt.
***Postreform III** (ab 1998):*
Das noch bestehende Monopol bei der Netzinfrastruktur und beim öffentlichen Telefondienst fällt weg, d.h. private Firmen oder auch kommunale Versorgungsunternehmen können Netzleistungen anbieten.

Die Aufgabe der **Datenschutzkontrolle** darf nicht - wie im diskutierten Gesetzesentwurf vorgesehen - einer Regulierungsbehörde zufallen, die nicht unabhängig ist und in Interessenskonflikte geraten kann. Statt dessen müssen unabhängige Stellen wie der Bundesbeauftragte für den Datenschutz zur Kontrolle des Telekommunikationsbereiches eingebunden werden.

Nicht nur der Entwurf für ein Telekommunikationsgesetz weist aus unserer Sicht Kritikpunkte auf. Die Verarbeitung personenbezogener Daten im Telekommunikationsbereich soll für die nächsten Jahre in einer neuen **„ Telekommunikationsdienstunternehmen - Datenschutzverordnung** (TDSV)" geregelt werden. Uns liegt ein Entwurf des Bundesministeriums für Post und Telekommunikation vor, der zu datenschutzrechtlichen Verschlechterungen gegenüber der jetzigen Situation führen würde.

- Ein **Einzelverbindungsnachweis** soll nun auch ohne das Einverständnis der zum Haushalt gehörenden Mitbenutzer des Anschlusses erteilt werden können.

- Außerdem dürfen Einzelverbindungsnachweise künftig auch mit **vollständigen Zielnummern** (ohne Verkürzung um die letzten drei Ziffern) erstellt werden. Dies ist ein Eingriff in das Recht auf informationelle Selbstbestimmung des Angerufenen, der keine Möglichkeit hat, die Aufnahme seiner Rufnummer in Einzelverbindungsnachweise anderer Teilnehmer zu verhindern. Die Datenschutzbeauftragten haben statt dessen vorgeschlagen, daß jeder Anschlußinhaber selbst entscheiden können sollte, ob und ggf. wie seine Rufnummer auf Einzelverbindungsnachweisen erscheint, so wie es z.B. in den Niederlanden praktiziert wird.

- Der Entwurf schränkt den Kreis der **Beratungsstellen** ein, deren Rufnummer nicht in Einzelverbindungsnachweisen aufgeführt werden soll. So ist die Möglichkeit beispielsweise für Personal- oder Betriebsräte sowie Frauenhäuser nicht vorgesehen.

- Obwohl die Regelungen über Bildschirmtextdienste Ländersache sind und dem BTX-Staatsvertrag entnommen werden können, enthält der Verordnungsentwurf davon abweichende Vorschriften. Demnach soll bei der Inanspruchnahme von **Bildschirmtextdiensten** das Erheben **zusätzlicher Daten** gestattet sein, die erst sechs Monate nach Erstellen der Rechnung gelöscht sein müssen, auch wenn sie für Abrechnungszwecke schon lange nicht mehr erforderlich sind.

Was ist zu tun?
Die Landesregierung sollte unsere Position im Bundesrat unterstützen.

7.3 Schleswig-Holstein-Netz

Ohne viel Aufhebens hat die Datenzentrale das Schleswig-Holstein-Netz etabliert. Es wird bereits von über hundert Behörden genutzt. Allerdings fehlt eine Dokumentation der Datenschutz- und Datensicherheitsmaßnahmen. Die Kunden können die Risiken nicht abschätzen.

Die Möglichkeit der Datenfernübertragung von Kunden der **Datenzentrale** Schleswig-Holstein zum dortigen Rechenzentrum gibt es schon lange. Früher mußten sich die Kunden über das Telefonnetz direkt bei der Datenzentrale einwählen oder aber Standleitungen mieten und konnten dann ihre Daten zur Weiterverarbeitung im Rechenzentrum übertragen.

Inzwischen hat die Datenzentrale mit eigenen Vermittlungsrechnern in mehreren Orten Schleswig-Holsteins neue Einwahlpunkte geschaffen, so daß die Kunden ihre Telefonverbindungen im Nahbereich zu günstigeren Tarifen aufbauen können. Aus der Sterntopologie mit der Datenzentrale in der Mitte ist eine hierarchische Struktur mit durch Vermittlungsrechner getrennten Ebenen geworden. Unter der Bezeichnung **Schleswig-Holstein-Netz** wird den Kunden nicht nur die Übertragung von Daten an das Rechenzentrum, sondern das elektronische Austauschen beliebiger Informationen, auch miteinander, ermöglicht. Die Datenzentrale plant, das Schleswig-Holstein-Netz zu einem Behördennetz auszubauen. Zum Beispiel könnten Behörden über das Netz elektronische Briefe (E-Mail) austauschen, Informationen bekanntgeben („elektronisches Amtsblatt") oder auch selbst recherchieren. Über Schnittstellen zu anderen Netzen sind weitere Anwendungen denkbar. Sogar auf Sprachübertragung und Videokonferenzen könnte das Netz ausgedehnt werden.

Stichwort
Schleswig-Holstein-Netz
Das Schleswig-Holstein-Netz ist ein landesweites Rechnernetz, das die Datenzentrale ihren Kunden zur Übertragung von Daten anbietet. Dazu werden Leistungen der Telekom genutzt, die durch eigene Vermittlungsrechner der Datenzentrale gebündelt sind. Es gibt Planungen, das Netz zu einem Behördennetz auszubauen.

Während bei der herkömmlichen Datenübertragung ausschließlich das Netz der Telekom beansprucht wurde, ergibt sich mit dem Schleswig-Holstein-Netz eine neue Situation. Wegen der fehlenden Zuständigkeit für die Telekom als bundesweites Wirtschaftsunternehmen hatten wir bislang keine andere Wahl, als auf die Datensicherheit der über die Telefonleitungen und Vermittlungsrechner übertragenen Informationen zu vertrauen. Mit der Etablierung des Schleswig-Holstein-Netzes sind nun **eigene Vermittlungsrechner der Datenzentrale** hinzugekommen, die die Daten aus dem Telekom-Netz herausnehmen und wiederum über Telefonleitungen an einen anderen Vermittlungsrechner weiterleiten.

Daraus ergeben sich eine Reihe von Fragen, etwa: Wie werden dort Vertraulichkeit und Datensicherheit der übertragenen Informationen garantiert? Welche Maßnahmen sind getroffen, um die Daten vor einem unbefugten Abhören und einem Verfälschen zu schützen und um sicherzustellen, daß sie beim Empfänger ankommen und nicht zu falschen Adressen weitergeleitet werden? Wie genau sehen die Einflußmöglichkeiten der Datenzentrale oder Dritter aus, wenn sich die Vermittlungsrechner in angemieteten Räumen anderer Behörden befinden? Ein umfassendes Konzept zum Datenschutz und zur Sicherheit beim Schleswig-Holstein-Netz konnte uns bislang noch nicht vorgelegt werden.

Bereits weit über hundert Behörden nutzen das neue Landesnetz. Sobald dort personenbezogene Daten übertragen werden, stellt sich das Schleswig-Holstein-Netz als Teil eines automatisierten Verfahrens dar und unterliegt demnach der **Datenschutzverordnung**. Dies bedeutet, daß die datenverarbeitenden Stellen, denen die Verantwortung für die ordnungsgemäße Datenverarbeitung obliegt, vor dem Einsatz das Verfahren testen und freigeben müssen. Beim Schleswig-Holstein-Netz ist dies den Behörden zur Zeit schlicht nicht möglich. Wegen der fehlenden Dokumentation der Datenschutz- und Datensicherheitsmaßnahmen können die Kunden nicht das Risiko einer Nutzung des Schleswig-Holstein-Netzes abschätzen.

Wir sind der Auffassung, daß es im Interesse einer technisch sauberen und kundenfreundlichen Entwicklung selbstverständlich sein sollte, frühzeitig - d.h. deutlich vor der Inbetriebnahme - **Datenschutz- und Sicherheitskonzepte** zu erstellen und den Kunden rechtzeitig auszuhändigen.

Es wäre zudem sinnvoll, wenn nicht jede Behörde einzeln die Systeme umfassend testen und freigeben müßte, sondern sich bis zu einem gewissen Grad auf **Zertifikate** verlassen könnte. Einen Anfang macht bereits die Automationskommission der Kommunen, die als Service für die Behörden diejenigen Softwareprodukte untersucht, die in größerem Maßstab eingesetzt werden, und Freigabeempfehlungen ausspricht. Umfassende Tests in professionellem Maßstab sind allerdings derzeit nicht möglich. Hierfür wären spezialisierte Mitarbeiter erforderlich, die sowohl im Vorfeld als auch während des Einsatzes von Produkten intensive Untersuchungen anstellen können.

Auch reicht es nicht aus, lediglich Softwareprodukte zu zertifizieren, wie man am Beispiel Schleswig-Holstein-Netz erkennt. Die Analysen und Freigabeempfehlungen müssen auf Systeme, bestehend aus Software, Hardware und Dienstleistungen, ausgedehnt werden. Bedingung dafür ist jedoch, daß der Anbieter der Systeme ihre Funktionsweise transparent für den Kunden darstellt und aussagekräftige Unterlagen mitliefert. Dies ist in einer Zeit, in der überall die Qualitätssicherung beschworen wird, leider eher die Ausnahme denn die Regel.

Was ist zu tun?
Die Datenzentrale sollte für das Schleswig-Holstein-Netz ein überzeugendes Sicherheitskonzept vorlegen.

7.4 Schöne neue ISDN-Welt bei Landtag und Regierung

Moderne Telefonanlagen erleichtern und beschleunigen die Kommunikation im Büro. Bei soviel neuer, bequemer Technik sollte auch Raum für den Datenschutz derer sein, die sie nutzen. Die neue Telefonanlage entspricht diesen Ansprüchen noch nicht.

Im Jahr 1995 erfolgte die Beschaffung und Installation einer komfortablen digitalen Telefonnebenstellenanlage (ISDN), die für die Landesdienststellen im Bereich Düsternbrook. Sie enthält eine Reihe bemerkenswerter technischer Leistungsmerkmale. Erst nach der Installation wurde die Frage an uns herangetragen, ob denn alle Funktionen des neuen Systems mit datenschutzrechtlichen Grundsätzen vereinbar seien. Eine datenschutzrechtliche Analyse ergab im wesentlichen **drei Problembereiche**, deren Erörterung bisher noch nicht abgeschlossen werden konnte:

- Bestimmten Apparaten kann eine **Direktrufmöglichkeit** zugeordnet werden. Mit ihr können andere Systemteilnehmer auf Knopfdruck unter Umgehung von Vorzimmerapparaten unmittelbar angerufen werden. Führt ein im Direktruf erreichbarer Teilnehmer ein Telefongespräch, so wird dies optisch durch eine Kontrollampe auf dem Apparat des anderen angezeigt, und zwar unabhängig davon, ob dieser im Moment überhaupt mit ihm telefonieren will. Daraus ergibt sich die **Möglichkeit der kontinuierlichen optischen Überwachung** des Telefonverhaltens der eingespeicherten Teilnehmer. Dies ist schon im Hinblick auf eigene weisungsgebundene Mitarbeiter problematisch, denn es dürfte mit dem Bild eines kooperativen Führungsverhaltens kaum vereinbar sein, wenn Vorgesetzte ständig das Telefonverhalten ihrer Mitarbeiter kontrollieren können. Wird aber eine Telefonanlage gemeinsam von Legislative und Exekutive genutzt, so ergeben sich brisante Probleme, die noch weit über den Datenschutz hinausgehen.

- Beim Zuschalten anderer Gesprächsteilnehmer (Konferenzschaltung), des Lautsprechers oder der Gesprächsabwicklung ohne Aufnehmen des Telefonhörers (frei sprechen) können Situationen auftreten, in denen das nichtöffentlich gesprochene Wort von anderen im Zimmer Anwesenden **mitgehört** wird. Dies kann unter Umständen sogar strafbar sein. Zwar soll in einer Dienstanweisung vorgeschrieben werden, daß die Aktivierung der entsprechenden Leistungsmerkmale dem jeweiligen Gesprächspartner mündlich mitgeteilt und dessen Einwilligung eingeholt werden muß. Um Abhilfe gegen versehent-

liche oder bewußt rechtswidrige Zuschaltungen zu schaffen, müßte jedoch beim Gesprächsteilnehmer ein **akustisches Signal** bei Aktivierung der betreffenden Funktionen automatisch ertönen.

- Außerdem war zu kritisieren, daß bisher noch **keine** klaren **Benutzungsregelungen** erlassen sind, sowohl was die Leistungsmerkmale als auch was die Verantwortlichkeit für das Funktionieren der Anlage betrifft. Schließlich handelt es sich bei der neuen Telefonanlage um ein **computergesteuertes Datenverarbeitungsverfahren**, in dem sensible personenbezogene Daten verarbeitet werden. Deshalb ist festzulegen, wer für das System (Steuerung, Verarbeitung der Daten, Datenschutz) zuständig ist, wer die Anlage in wessen Auftrag technisch wartet und wer die **datenschutzrechtliche Verantwortung** für die gespeicherten Daten trägt. Außerdem sind etwaige Verträge über die Verarbeitung der Daten im Auftrag schriftlich und unter Einhaltung der einschlägigen Bestimmungen des Landesdatenschutzgesetzes abzuschließen .(z.B. ist zu klären, an wen sich Betroffene zur Geltendmachung ihrer datenschutzrechtlichen Ansprüche auf Auskunft, Löschung etc. wenden können oder wer ggf. eine richterlich genehmigte Abhörmaßnahme realisieren muß).

Die bisherigen Reaktionen des **Innenministeriums** waren nicht zufriedenstellend. Zwar wurde mitgeteilt, der Direktruf werde nur eingerichtet, wenn die Betroffenen zugestimmt haben; die Einzelheiten des Verfahrens bedürfen aber noch der Klärung. Ein akustisches oder optisches Signal bei Einschaltung des Lautsprechers sei nach Angaben der Herstellerfirma nicht möglich. Nun sollen in einer Dienstanweisung entsprechende Regelungen getroffen werden. Bis zur Erstellung dieses Berichts wurde weder eine klare Benutzungsregelung noch eine den gesetzlichen Anforderungen genügende Dateibeschreibung vorgelegt. Insgesamt ist es enttäuschend, daß eine so aufwendige moderne Telefonanlage zwar eine Fülle von Leistungsmerkmalen enthält, wichtige Funktionen zum optimalen Schutz der Grundrechte der Benutzer aber technisch nicht möglich sein sollen.

Was ist zu tun?
Der Innenminister sollte die datenschutzrechtlichen Mängel der neuen Telefonanlage umgehend beheben.

7.5 Elektronische Geldbörsen dürfen keine Datenspuren hinterlassen

Chipkarten werden künftig das Bargeld teilweise ersetzen. Zu den bisherigen kartengestützten Zahlungssystemen kommt die elektronische Geldbörse. Es muß sichergestellt werden, daß das elektronische Geld im gleichen Maße wie Bargeld anonym ausgegeben werden kann.

Bargeld ist unmodern geworden - immer mehr Geschäfte bieten ihren Kunden an, elektronisch „per Karte" zu bezahlen. Während Kredit- und Eurocheque-Karte (ec-Karte) eher für größere Beträge gedacht sind, lassen sich geringe Kosten bisher nur bei wenigen Anbietern kartengestützt begleichen, z.B. mit der Telefonkarte. Hier soll die **elektronische Geldbörse**, eine Chipkarte mit Zahlungsfunktion, Abhilfe schaffen. Ihr Einsatz ist spätestens ab 1997 geplant. Auch die ec-Karten, die Ende 1996 ausgegeben werden, sollen nach Planung der deutschen Banken dann zu diesem Zweck mit einem Chip versehen sein, in dem ein Guthaben gespeichert wird.

Stichwort Elektronische Geldbörse
Elektronische Geldbörsen sind Chipkarten, auf denen sich ein Guthaben einspeichern läßt und die anstelle von Bargeld eingesetzt werden können. Beim Einkaufen wird von der elektronischen Geldbörse die entsprechende Summe abgebucht. An besonderen Automaten läßt sich die Chipkarte erneut mit Geld auffüllen.

Von diesem Betrag wird beim Bezahlen mit der elektronischen Geldbörse die zu begleichende Summe direkt abgezogen, ohne daß wie bei anderen Karten eine Geheimzahl einzugeben oder ein Beleg zu unterschreiben ist oder daß wie bei Barzahlung Wechselgeld herausgegeben werden muß. Das Bezahlen soll zwei bis drei Sekunden dauern oder beim Einsatz von kontaktlosen Chipkarten, die im Vorbeigehen ausgelesen werden können, sogar noch schneller vonstatten gehen.

Im Gegensatz zum Bezahlen mit Bargeld hinterläßt man beim Benutzen einer Kredit- oder ec-Karte **elektronische Spuren**, die Informationen darüber beinhalten, wieviel Geld man wann wo ausgegeben hat. Zu Abrechnungszwecken werden nämlich alle Buchungen gespeichert und mindestens sechs Jahre lang aufbewahrt. Wenn auf diese Weise kleine Beträge überall elektronisch bezahlt werden, droht die Gefahr, daß die vielen Spuren zu detaillierten **Bewegungs- und Konsumprofilen** verdichtet werden, die auf reges Interesse bei Marketingleuten, Polizei, Staatsanwaltschaft, Finanzämtern oder auch Arbeitgebern stoßen könnten.

Dagegen ist es bei Guthabenkarten (**Pre-Paid-Karten**) nicht notwendig, überhaupt personenbezogene Daten zu erheben. Verschiedene Modelle, die sich hauptsächlich in ihrem Abrechnungsverfahren und der Menge der zu diesem Zweck benötigten Daten unterscheiden, werden zur Zeit

erprobt. Welcher Chipkartentyp zur deutschen elektronischen Geldbörse wird, steht noch nicht fest. Als „Cartemonnaies“ kommen in Frage:

- Guthabenkarten, zu denen ein kartenbezogenes „Schattenkonto“ geführt wird: Es werden Stellen zur branchenübergreifenden Verrechnung (sog. Clearing) der einzelnen Zahlungsvorgänge eingeführt. Jede Änderung des Kartenguthabens durch Aus- oder Einzahlung wird auf einem Verrechnungskonto der **Clearing-Stelle** gebucht. Dadurch soll eine größere Sicherheit gegen Betrüger und Hacker erreicht werden. Außerdem geht das Geld einer defekten Karte nicht verloren.

- **Guthabenkarten ohne Clearing**: Diese Karten kommen einer Geldbörse am nächsten, da kein Verrechnungskonto existiert. Die Zahlungen werden lediglich auf dem Chip verbucht; Einzelbeträge werden nicht nach ihrer Herkunft unterschieden. Der Karteninhaber kann sich die zuletzt getätigten Transaktionen anzeigen lassen. Zu diesem Kartentyp gehört die britische Entwicklung „Mondex“, mit der Geld auch von Karte zu Karte übertragen werden kann.

- Guthabenkarten mit Clearing und ohne Schattenkonten: Die **Verrechnungsstellen** organisieren den Geldtransfer, führen jedoch kein kartenbezogenes Konto.

Da Clearing-Verfahren mit Schattenkonten einen Personenbezug über die Nummer des Verrechnungskontos ermöglichen, sind rein anonyme Zahlungsmethoden zu bevorzugen. Gemeinsam mit den anderen Datenschutzbeauftragten des Bundes und der Länder fordern wir, daß als elektronische Geldbörse nur solche Guthabenkarten eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen. Auch in Zukunft muß eine **anonyme Teilnahme am wirtschaftlichen Leben** im gleichen Umfang wie bisher mit Bargeld möglich sein.

8. Europa

8.1 EU-Datenschutzrichtlinie

Nach langjährigen Verhandlungen ist 1995 die Europäische Datenschutzrichtlinie verabschiedet worden. Sie wird Auswirkungen vor allem auf die Zulässigkeit der Datenverarbeitung durch Private und auf Datenübermittlungen in Staaten außerhalb der EU haben.

Die EU-Datenschutzrichtlinie schafft ein einheitlich **hohes Datenschutzniveau** innerhalb der Europäischen Union. Mit diesem Schutzzweck für den einzelnen wird aber auch gleichzeitig das Ziel eines freien Datenverkehrs innerhalb der EU verbunden. Die Richtlinie erkennt allerdings an, daß es auch weiterhin datenschutzrechtliche Regelungsunterschiede innerhalb der Gemeinschaft geben kann, auch wenn sie sich auf den Datenverkehr zwischen den Mitgliedstaaten auswirken: Sie bietet den Mitgliedstaaten an verschiedenen Stellen Regelungsvarianten an, die im Ergebnis, nicht jedoch in ihren Mitteln ein gleiches Schutzniveau gewährleisten sollen. Darüber hinaus fordert die Richtlinie die Mitgliedstaaten auf, ihren **Umsetzungsspielraum** zu einer **Verbesserung** ihres **gegenwärtigen Datenschutzniveaus** zu nutzen. Die Umsetzung der EU-Richtlinie sollte deshalb als Chance zur Anpassung des deutschen Datenschutzrechts an die technische Fortentwicklung und die gesellschaftlichen Probleme der modernen Datenverarbeitung genutzt werden.

- Anders als bislang das deutsche Datenschutzrecht unterscheidet die EU-Richtlinie nicht zwischen der Datenverarbeitung durch öffentliche Stellen und durch **Private**. Angesichts der wachsenden Bedeutung privater Datenverarbeitung ist es längst überfällig, daß künftig auch für diesen Bereich strengere datenschutzrechtliche Voraussetzungen wie die Zweckbindung der Daten und die Erforderlichkeit der Datenverarbeitung gelten werden.

- Besonders strenge Voraussetzungen werden an die Verarbeitung von **hochsensiblen personenbezogenen Daten** wie ethnische Herkunft, weltanschauliche und politische Überzeugung, Gesundheit und Sexualleben gestellt. Beispielsweise ist eine Verarbeitung von Gesundheitsdaten nur durch Personen zulässig, die dem ärztlichen Berufsgeheimnis unterliegen.

- Die Richtlinie verbietet es, daß **bewertende Einzelentscheidungen** zu einer Person ohne deren Anhörung allein auf der Grundlage einer automatisierten Datenverarbeitung ergehen.

- Datenverarbeitungen, die spezifische Risiken für das Persönlichkeitsrecht aufweisen, müssen **vorab** eine interne oder externe datenschutzrechtliche **Kontrolle** durchlaufen.

- Neben dem Recht auf Auskunft über seine Daten hat der Betroffene grundsätzlich das Recht, aufgrund besonderer Umstände einer Datenverarbeitung zu **widersprechen**.

- Personenbezogene Daten dürfen nur in solche **Drittstaaten** außerhalb der EU übermittelt werden, die ein **„angemessenes Schutzniveau"** gewährleisten. Im Wege der gegenseitigen Konsultation und über ein Ausschußverfahren verständigen sich die Mitgliedstaaten darüber, bei welchen Drittstaaten diese Voraussetzung vorliegt. Ausnahmen läßt die Richtlinie allerdings zu, wenn beispielsweise vertraglich ausreichende Datenschutzgarantien zugesichert werden.

- Die Mitgliedstaaten haben die Möglichkeit, Ausnahmen von der Pflicht zur Meldung von Datenverarbeitungen gegenüber einer öffentlichen Kontrollstelle vorzusehen, wenn innerhalb der öffentlichen oder privaten datenverarbeitenden Stelle eine unabhängige Überwachung durch einen Datenschutzbeauftragten stattfindet. Neben dem **betrieblichen Datenschutzbeauftragten** nach dem Bundesdatenschutzgesetz könnte hierdurch die Institution eines **behördlichen Datenschutzbeauftragten** ausgebaut werden.

- Die **öffentlichen Datenschutzkontrollinstitutionen** sollen ihre Aufgaben in **„völliger Unabhängigkeit"** und auch im privaten Bereich anlaßunabhängig wahrnehmen. Als wirksame Instrumente zur Durchsetzung des Datenschutzrechts sieht die Richtlinie u.a. die Möglichkeit unmittelbarer Anordnungsbefugnisse, eines Klagerechts und Anzeigebefugnisse bei datenschutzrechtlichen Verstößen vor.

Insgesamt bietet die allgemeine Datenschutzrichtlinie der EU durch ihr **beachtliches Schutzniveau** und durch ihre **flexible Regelungstechnik** eine gute Grundlage für die Modernisierung des deutschen Landes- und Bundesdatenschutzrechts. Sie bekräftigt den Anspruch, daß eine europäische, ja eine weltweite Informationsgesellschaft mit entsprechenden, der Datenverarbeitungstechnik angemessenen Sicherungen des Persönlichkeitsrechts einhergehen muß. Die bereichsspezifische Verwirklichung dieses Anspruchs bleibt allerdings auf Ebene der Europäischen Union weiterhin eine wesentliche Herausforderung. Die EU-Richtlinie ist innerhalb von drei Jahren in innerstaatliches Recht umzusetzen.

Was ist zu tun?

Der Schleswig-Holsteinische Landtag muß das Landesdatenschutzgesetz an die Richtlinie anpassen.

8.2 Entwurf einer Telekommunikationsrichtlinie

Auch im vergangenen Jahr hat es keine Einigung über den Vorschlag einer EU-Richtlinie zum Datenschutz in digitalen Telekommunikationsnetzen gegeben. Statt dessen wurden jedoch Regelungen zur Öffnung der Sprachtelefondienstnetze vorangetrieben, die ihrerseits keine datenschutzrechtlichen Bestimmungen enthalten.

Bis zum 01.01.1998 sollen die Telekommunikationsdienste und - infrastruktur innerhalb der Europäischen Union für den Wettbewerb geöffnet werden. (vgl. auch Tz. 7.2) In Vorbereitung auf diese Liberalisierung hat die Europäische Kommission 1995 Richtlinienvorschläge zur Gewährleistung **eines offenen Netzzugangs in der Telekommunikation** vorgelegt. Darin werden die Anforderungen an die Bereitstellung von Telekommunikationsdiensten, an die Nutzung von Netzen und deren Zusammenschaltung geregelt, um eine Interoperabilität der Dienste und eine weitgehende Netzsicherheit zu gewährleisten. Einheitliche Bedingungen für den Wettbewerb auf dem europaweiten Markt für Telekommunikationsgeräte und -dienste setzen aus unserer Sicht aber auch eine europaweite Gewährleistung des informationellen Selbstbestimmungsrechts in der Telekommunikation voraus. Hierzu verweisen die genannten Regelungsvorschläge jedoch lediglich auf anderweitige Rechtsvorschriften über den Datenschutz.

Andererseits wurde das Vorhaben der EU, eine Richtlinie über den **Datenschutz in digitalen Telekommunikationsnetzen** (insbesondere ISDN) zu verabschieden, im letzten Jahr **zurückgestellt**, während die Vorhaben zur **Liberalisierung** der Telekommunikationsdienste und -netze mit erkennbarer Priorität **vorangetrieben** wurden. Es droht daher eine Schieflage, wenn durch die Liberalisierung der Telekommunikation die entscheidenden Planungen und Investitionen der betreffenden Marktteilnehmer bereits festgelegt werden, bevor die entsprechenden europaweiten, für alle Wettbewerber verbindlichen Datenschutzregeln in der Telekommunikation bekannt sind. Die europäischen Datenschutzbeauftragten haben daher für eine inhaltliche Harmonisierung und eine parallele Beratung der verschiedenen Richtlinienvorhaben im Telekommunikationsbereich plädiert.

Die spanische Präsidentschaft legte im November 1995 einen im wesentlichen redaktionell, nur an wenigen Stellen inhaltlich geänderten Entwurf der Telekommunikationsrichtlinie vor. Es bleibt demnach bei der in unserem letzten Tätigkeitsbericht (17. TB, Tz. 7.1) dargestellten Forderung nach einer raschen Verabschiedung einer europäischen Telekommunikations-Datenschutzrichtlinie auf hohem Schutzniveau.

Was ist zu tun?
Die Landesregierung sollte unsere Position bei den Verhandlungen über die europäische Telekommunikationsrichtlinie unterstützen.

8.3 Vorbereitung auf Maastricht II

Bei der 1996 stattfindenden Regierungskonferenz zur Revision der Europäischen Unions- und Gemeinschaftsverträge muß auch der Datenschutz berücksichtigt werden. Die europäischen Datenschutzbeauftragten haben hierfür eine Reihe von Vorschlägen formuliert.

Obwohl in der Arbeit der EU personenbezogene Daten in beträchtlichem Ausmaß entstehen (z.B. in der Statistik, Agrar- oder Zollverwaltung) und die EU Entwicklungen zum Ausbau internationaler Kommunikationsnetze und von Informationstechnologien vorantreibt, fehlt in den **EU-Verträgen** ein ausdrücklicher Hinweis auf den Datenschutz. Angesichts der hohen wirtschaftlichen und gesellschaftlichen Bedeutung, die der Weiterentwicklung von Informations- und Kommunikationstechnologien durch Mitgliedstaaten und Organe der EU selbst beigemessen wird, ist es höchste Zeit, diese Lücke zu schließen. Die Datenschutzbeauftragten des Bundes und der Länder und die europäischen Datenschutzbeauftragten haben Ende 1995 jeweils gemeinsame Entschließungen gefaßt, um eine Berücksichtigung des Datenschutzes bei der Vertragsrevisionskonferenz 1996 („Maastricht II") zu erreichen:

Stichwort Maastricht II
Der 1992 in Maastricht geschlossene Vertrag über die Europäische Union sieht für 1996 eine weitere Regierungskonferenz vor, auf der über eine Revision des Maastrichter Vertragswerkes beraten werden soll. Möglicher Verhandlungsgegenstand ist auch die Stärkung des Grundrechtsschutzes innerhalb der EU.

- Im Rahmen eines **Grundrechtskataloges** des EU-Vertrages sollte ein für den einzelnen **einklagbares, ausdrückliches Recht auf Datenschutz** verankert werden, das für die Organe der Union und für die Mitgliedstaaten, soweit sie Gemeinschaftsrecht ausführen, einen einheitlichen Maßstab für die Beachtung der Persönlichkeitsrechte auf hohem Schutzniveau garantiert. Für den Bürger ergäbe sich eine gerichtlich durchsetzbare Garantie für die Beachtung seiner Privatsphäre auch in einer multimedialen Informationsgesellschaft. Damit wäre im übrigen eine datenschutzrechtliche Gleichstellung der europäischen Wettbewerber erreicht.

- Unabhängig hiervon müssen rechtsverbindliche Datenschutzregelungen für die **Organe** und **Einrichtungen der EU** geschaffen werden, wie dies bereits ein inzwischen nicht weiterverfolgter Vorschlag der Europäischen Kommission von 1990 vorsah.

- Die Verträge müssen eine **unabhängige europäische Datenschutzkontrollinstanz** vorsehen, an die sich einzelne Bürger wenden können, die aber auch anlaßunabhängige Prüfrechte, Beratungs- und Beteiligungskompetenzen hat.

Nur durch eine vertragliche Gewährleistung kann erreicht werden, daß künftig in den unterschiedlichen Bereichen der EU (z.B. Telekommunikation, Forschungsförderung, Inneres und Justiz, Arbeitnehmerrechte) ausreichende bereichsspezifische Datenschutzregelungen getroffen werden. In einem weiter zusammenwachsenden Europa ist es schließlich von großer Bedeutung, daß alle Mitgliedstaaten, auch wenn sie bisher kaum Datenschutzregelungen kannten, die Persönlichkeitsrechte beachten.

Was ist zu tun?

Die Landesregierung sollte unsere Vorschläge bei den Beratungen über Maastricht II unterstützen.

9. Was es sonst noch zu berichten gibt

9.1 Woran der Datenschutz nicht schuld war

Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn dafür entweder eine Rechtsvorschrift oder die Einwilligung der Betroffenen als Befugnisgrundlage vorhanden ist. Bereits im letzten Tätigkeitsbericht (17. TB, Tz. 4.1.1.3) hatten wir darauf hingewiesen, daß diese Maßgabe auch für den Austausch von **Vergleichsmitteilungen** zur **Festsetzung des Ortszuschlages** bei Mitarbeitern im öffentlichen Dienst gilt. Allerdings waren wir auch der Auffassung, Vergleichsmitteilungen seien ohnehin in den meisten Fällen überflüssig, da jeder Arbeitgeber für sich die Anspruchsvoraussetzungen für die Zahlung des Ortszuschlages zu prüfen hat. Der Betroffene hat dazu ggf. entsprechende Nachweise über die Besoldung bzw. Vergütung seines Ehegatten vorzulegen.

Das Landesbesoldungsamt konnte sich dieser Auffassung offensichtlich nicht anschließen. Jedenfalls wurden alle verheirateten Mitarbeiter des Landes - unabhängig davon, ob der Ehegatte überhaupt beschäftigt war - angeschrieben und vorsorglich um ihre Einwilligung zum Austausch von Vergleichsmitteilungen gebeten. Dabei konnte bei den Betroffenen durchaus der Eindruck entstehen, dies geschehe auf unsere Veranlassung, weil, wie es in dem Schreiben heißt, „der Landesbeauftragte für den Datenschutz es für erforderlich hält, daß für den Austausch derartiger Vergleichsmitteilungen die freiwillig erteilte Einwilligung der Betroffenen vorliegt".

Um dies hier noch einmal klarzustellen: Wir halten den Austausch von Vergleichsmitteilungen, von wenigen Ausnahmefällen abgesehen, für nicht erforderlich.

Auch bei den **Betroffenen** ist die Aktion auf **Unverständnis** gestoßen. In den meisten Eingaben, die uns in dieser Sache erreicht haben, wurde danach gefragt,

- weshalb überhaupt ein zusätzlicher Datenabgleich durchgeführt werden soll, wo doch das Landesbesoldungsamt schon alle erforderlichen Nachweise erhalten hat, und

- wozu die Einwilligung benötigt wird, wo doch das Landesbesoldungsamt weiß, daß der Ehegatte gar nicht beschäftigt ist. Teilweise wurde auch die Vermutung geäußert: „oder haben die nichts Wichtigeres zu tun?"

Da wir keine plausiblen Antworten auf die gestellten Fragen parat hatten, konnten wir die Betroffenen nur darauf hinweisen, daß die Teilnahme an der Aktion ausschließlich freiwillig erfolgt.

9.2 Darf die Ehefrau eines Lehrers zu Hause Schulzeugnisse schreiben?

In einer Schule wurden die Zeugnisse der Schüler von einer nicht an der Schule beschäftigten Person, und zwar von der Ehefrau des stellvertretenden Schulleiters, zu Hause geschrieben. Vertragliche Regelungen waren mit ihr nur unvollkommen und überdies nur mündlich getroffen worden. Erst auf unsere weitergehende Nachfrage stellte sich heraus, daß sie de facto für den Schulträger die Funktion der Schulsekretärin ausübte. Wir haben den Schulleiter darauf hingewiesen, daß zur rechtlichen Absicherung der Tätigkeit als Schulsekretärin ein schriftlicher Arbeitsvertrag geschlossen werden sollte, in dem insbesondere auch die Verschwiegenheitspflicht als Vertragsbestandteil geregelt wird. Daneben ist die Mitarbeiterin durch den Schulträger über die Datenschutzvorschriften im Sinne des Landesdatenschutzgesetz zu unterrichten. Ferner ist dafür Sorge zu tragen, daß die zu Hause verarbeiteten personenbezogenen Daten ausreichend vor der Einsichtnahme Unbefugter geschützt werden. Uns wurde inzwischen der Abschluß eines entsprechenden Vertrages mit einer Schulsekretärin mitgeteilt.

9.3 Wenn zwei Polizeibeamte sich streiten

Zwischen zwei Polizeibeamten war es außerhalb ihres Dienstes zu Handgreiflichkeiten gekommen. Beide Beteiligte erstatteten wechselseitige Strafanzeigen. Die Ermittlungsverfahren wurden mangels öffentlichen Interesses eingestellt. Daraufhin erstattete der Dienstvorgesetzte eines der beiden Kontrahenten **Dienstaufsichtsbeschwerde** gegen den anderen beteiligten Polizeibeamten bei dessen Dienstvorgesetzten und fügte u.a. die von jenem erstattete Strafanzeige bei. Unsere Nachprüfung ergab, daß eine Rechtsgrundlage für die zweckändernde Verwendung von Strafanzeigen für Zwecke eines Disziplinarverfahrens nicht besteht. Die vorgesetzte Dienststelle hat den datenschutzrechtlichen Verstoß eingeräumt und die Strafanzeige aus dem Disziplinarvorgang entfernt.

10. Rückblick

10.1 Innenminister sagt ggf. eigene Rechtstatsachensammelstelle für Schleswig-Holstein zu

Eine von den Innenministern beschlossene Rechtstatsachensammelstelle zur Überprüfung des polizeilichen Instrumentariums zur Straftatenbekämpfung ist inzwischen beim BKA eingerichtet worden (vgl. 17. TB, Tz. 4.1.2.1). Es bestehen erhebliche Zweifel, ob diese Stelle die Wirksamkeit und Verhältnismäßigkeit von Grundrechtseingriffen bei der Strafverfolgung objektiv bewerten möchte. Nach wie vor ist in erster Linie an die Sammlung spektakulärer Einzelfälle gedacht, in denen Rechtsvorschriften „hinderlich" waren.

Der schleswig-holsteinische Innenminister hat die Durchführung einer eigenen Rechtstatsachensammlung und -auswertung für das Land Schleswig-Holstein im Rahmen der Erörterung unseres letzten Tätigkeitsberichtes im Innen- und Rechtsausschuß in Aussicht gestellt. Daß er dabei auf eine wissenschaftliche Begleitung der eigenen Rechtstatsachensammlung besonderen Wert legen möchte, begrüßen wir. Wir werden uns an der weiteren Planung des Vorhabens, insbesondere hinsichtlich des Themenzuschnitts und der Bewertungskriterien, beteiligen; denn bevor stets neue Eingriffsbefugnisse beschlossen werden, muß erst geprüft werden, was die bisherigen Erweiterungen des Ermittlungsinstrumentariums gebracht haben.

10.2 Asylcard: Pläne noch nicht ad acta gelegt

1994 haben wir gegenüber dem Innenminister technische und verfassungsrechtliche Vorbehalte gegen die Konzeption einer „Asylcard" erhoben (vgl. 17. TB, Tz. 4.1.3.4) und ihn gebeten, unsere Bedenken in der weiteren Diskussion zu berücksichtigen. Diesem Wunsch hat der Innenminister entsprochen und dem federführenden Bundesinnenminister mitgeteilt, daß er die Durchführung einer „Machbarkeitsstudie" für eine Asylcard aus praktischen und verfassungsrechtlichen Gründen ablehne.



Der Bund und acht Länder haben sich allerdings für weitere Untersuchungen eingesetzt. Die Entscheidung über das weitere Vorhaben ist noch nicht gefallen.

10.3 Denkmalschutzgesetz verabschiedet

Nachdem mit dem Wissenschaftsministerium Einvernehmen über eine datenschutzgerechte Neugestaltung des Denkmalschutzgesetzes erzielt werden konnte, erwarteten wir Ende 1993 eine baldige Verabschiedung

des neuen Gesetzes. Wir hatten auf die Notwendigkeit einer Anpassung an das Datenschutzrecht schon früher aufmerksam gemacht (vgl. 9. TB, Tz. 4.6.3). Unser Hinweis schloß 1994 (vgl. 16. TB, Tz. 8.) mit der Forderung, die Vorarbeiten konsequent und zügig abzuschließen und das Gesetzgebungsverfahren einzuleiten. Das ist inzwischen geschehen. Das Gesetz wurde am 21.02.1996 verabschiedet.

10.4 Vorerst keine elektronische Autobahnmaut für Pkw

Im 16. Tätigkeitsbericht (Tz. 4.5.1) hatten wir unsere Bedenken bezüglich der automatisierten Erhebung von Straßenbenutzungsgebühren zusammengefaßt: Es würden personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet, aus denen sich exakte Bewegungsprofile erstellen ließen. Deshalb hatten wir gefordert, nur solche Zahlungssysteme einzusetzen, die keine Daten über ordnungsgemäß zahlende Verkehrsteilnehmer erheben und die Abrechnungsdaten dezentral und transparent für den Zahlenden speichern würden.

Nach einer Verlautbarung des Bundesverkehrsministers ergab sich nun aus Feldversuchen, daß Pkw zwar erfaßt, aber nur mit einem enormen und datenschutzrechtlich bedenklichen Aufwand kontrolliert werden können. Aus diesem Grund verzichte die Bundesregierung auf eine Autobahngebühr für Personenwagen. Allerdings würden im Jahre 2000 streckenbezogene Kosten für Lastkraftwagen sollen eingeführt werden, bei denen die Regierung geringere Kontrollprobleme sieht. Unklar ist jedoch, ob diese Lkw-Maut als Rechtfertigung für die Installation einer bundesweiten Registrierungsinfrastruktur dienen soll, die dann „auf Knopfdruck“ auch für andere Zwecke genutzt werden kann. Schließlich sind die Kfz-Kennzeichen auch deshalb neu gestaltet worden, um ihre Maschinenlesbarkeit (optische Erkennung) zu verbessern.

10.5 Datenverarbeitung bei der Suchtberatung neu organisiert

Im vorangegangenen Tätigkeitsbericht hatten wir die Prüfung einer Suchtberatungsstelle geschildert (s. 17. TB, Tz. 4.8.3). Dort war eine unzureichende Abschottung der Vorgänge des Suchtberaters gegenüber anderen Akten festgestellt worden. Der Träger dieser Beratungsstelle hat zwischenzeitlich mitgeteilt, die Akten des Sozialpsychiatrischen Dienstes seien insgesamt neu geordnet worden. Akten, die ausschließlich auf der Basis freiwilliger Beratungen entstanden seien - also die Mehrzahl der Suchtberatungsfälle - würden künftig getrennt von anderen Vorgängen aufbewahrt. Ferner seien aus der Kartei „Psychisch Kranke und Süchtige“, diejenigen Karteikarten, die freiwillige Beratungen und Betreuungen betreffen, entfernt worden. Ergänzend ist eine „Dienstanweisung über Datenerhebung, Datenspeicherung, Datensicherheit, Datenübermitt-

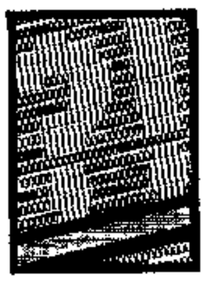
lung und Datenlöschung“ erlassen worden, die im wesentlichen unsere Zustimmung gefunden hat.

10.6 Bundesgrenzschutz als verlängerter Arm der Geheimdienste

In unserem 16. Tätigkeitsbericht (Tz. 4.1.2.1) haben wir herausgestellt, daß eine 1992 in Kraft getretene Dienstanweisung für den Bundesgrenzschutz mit den Verfassungsschutzgesetzen nicht in Einklang stand, weil sie den Grenzschutzbeamten Befugnisse suggeriert, die sie rechtlich gar nicht haben. So war aufgrund dieser Regelungen nicht auszuschließen, daß der Bundesgrenzschutz über das für die Grenzkontrolle notwendige Maß hinaus Bürger beobachtete und diese Informationen an die Geheimdienste weiterleitete.

Diesen Bedenken hat sich nunmehr die Parlamentarische Kontrollkommission des Deutschen Bundestages angeschlossen. Auf ihren Wunsch hin ist zwischenzeitlich eine Neufassung dieser Dienstanweisung erarbeitet worden, die mögliche Fehlauslegungen, wie sie bei der alten Fassung zu befürchten waren, ausschließt. Durch den ausdrücklichen Hinweis, daß „Ersuchen keine Rechtsgrundlage für die Erhebung von Informationen“ sind, wird klargestellt, daß diese interne Verwaltungsvorschrift keine eigenständige Befugnisgrundlage für eine Datenerhebung sein kann.

11. DATENSCHUTZAKADEMIE



Das Jahresprogramm 1996 ist gegenüber dem Vorjahr erneut fortgeschrieben worden, so daß die DATENSCHUTZAKADEMIE nunmehr zu 22 unterschiedlichen Themen insgesamt 28 Kurse, Seminare und Workshops anbietet. Da die Inhalte jährlich neu festgelegt werden, kann die DATENSCHUTZAKADEMIE auf aktuelle Entwicklungen rasch reagieren. So ist im Hinblick auf die zu erwartenden neuen gesetzlichen Bestimmungen das Angebot zum Thema „Personaldatenverarbeitung" ausgeweitet worden. Erstmals wird wegen der vom Justizminister angekündigten enormen Investitionen im Bereich der Automatisierung der Gerichte ein Seminar zum Thema „Datenschutz bei der Justiz" angeboten.

Die DATENSCHUTZAKADEMIE finanziert sich aus den Teilnehmerbeiträgen und hat sich zum Ziel gesetzt, ihre Dienstleistungen kostendeckend und marktgerecht anzubieten.

Kurse/Seminare/Workshops 1996

Kurse/Seminare/Workshops	Kurzbez.	Zeit	Ort
Datenschutz an der Schule	L 5	26.02.-27.02.1996	Leck
Schutz von Personaldaten	P 2	26.02.-27.02.1996	Bordesholm
Datenschutz im Bauamt	B 1	11.03.-12.03.1996	Leck
Datenschutzverordnung des Landes Schleswig-Holstein	VO 4	21.03.-22.03.1996	Leck
Seminar: Führung von Personalakten	PA 2	25.03.-26.03.1996	Bordesholm
Einführungskurs für Schulsekretärinnen	ES 1	11.04.1996	Bordesholm
Datenschutz an der Schule	L 6	25.04.1996	Kiel
SGB-Änderungsgesetz	SG 2	06.05.-08.05.1996	Leck
Workshop für Sozialdatenschutzbeauftragte	SW 1	08.05.-09.05.1996	Leck
Einstieg in das Datenschutzrecht	E 2	31.05.1996	Kiel
Beauftragte für Sozialdatenschutz	S 4	10.06.-14.06.1996	Leck
Datenschutz an der Schule	L 7	08.08.1996	Kiel

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
Schutz von Personaldaten	P 3	15.08.-16.08.1996	Bordesholm
Datenschutz an der Schule	L 8	29.08.-30.08.1996	Leck
Einführungskurs für Mitarbeiterinnen und Mitarbeiter von Ausländerbehörden	EA 1	02.09.1996	Kiel
Behördliche Datenschutzbeauftragte	D 6	02.09.-06.09.1996	Leck
Workshop für behördliche Datenschutzbeauftragte	DW 1	09.09.-10.09.1996	Leck
Datenschutz im Ordnungsamt	O 2	10.09.-11.09.1996	Leck
Datenschutz an der Schule	L 9	12.09.-13.09.1996	Leck
Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 2	12.09.-13.09.1996	Bordesholm
Seminar: Führung von Personalakten	PA 3	23.09.-24.09.1996	Bordesholm
Einführungskurs für Mitarbeiterinnen und Mitarbeiter von Verkehrsbehörden	EV 1	01.10.1996	Kiel
Workshop zur Datensicherheit	SIW 1	28.10.-29.10.1996	Leck
Datenschutz bei der Justiz	J 1	04.11.-08.11.1996	Leck
Datenverarbeitungsrecht für Führungskräfte in der Verwaltung	F 5	11.11.-13.11.1996	Leck
Datenschutz im Bereich der Umweltverwaltung	U 2	14.11.-15.11.1996	Leck
Seminar: Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	SI 2	02.12.-04.12.1996	Leck
Seminar: Revisionsfähigkeit der automatisierten Datenverarbeitung	R 2	09.12.-11.12.1996	Leck

Das Jahresprogramm '96 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN mit näheren Informationen zu den Veranstaltungen und Anmeldeformularen kann kostenlos angefordert werden beim

Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1208, Telefax: 0431/988-1223
E-Mail: ldsh@netzservice.de

12. Sommerakademie 1996

Am 26. August 1996 veranstaltet die DATENSCHUTZAKADEMIE im Landeshaus in Kiel die Sommerakademie 1996 zu folgendem Thema:

Datenschutz durch Technik
- Technik im Dienste der Grundrechte -

Zweifellos birgt die moderne Datenverarbeitungstechnik Gefahren für das Recht auf informationelle Selbstbestimmung. Inwieweit hält sie selbst Mittel bereit, diesen Gefahren entgegenzuwirken? Würden Computer personenbezogene Daten von vornherein nicht speichern oder selbsttätig zum frühestmöglichen Zeitpunkt wieder löschen, bedürfte es nicht komplizierter Rechtsregeln zu ihrem Schutz. Würden Daten sicher verschlüsselt übertragen, könnte der Aufwand zum Schutz der Übertragungswege dem Rechnung tragen. Könnten Chipkartensysteme zu einem Instrument der Gestaltung des informationellen Selbstbestimmungsrechts ausgestaltet werden, würde ihnen mit weniger Mißtrauen begegnet.

Die Sommerakademie 1996 bietet die Möglichkeit, diese Themen zu diskutieren. In Vorträgen und Diskussionen sollen Wissenschaftler, Politiker, Vertreter der Industrie, des Datenschutzes und von Verbraucherschutzorganisationen der Frage nachgehen, welche „grundrechtsfreundlichen" Techniken es bereits gibt und wo sie sinnvoll eingesetzt werden könnten.

PROGRAMM

09.00 - 12.00	Vorträge von Rednern aus den Bereichen Politik, Wissenschaft, Verbraucherschutz, Industrie und Datenschutz
13.00 - 15.30	Foren mit Vorträgen und Podiumsdiskussion zu folgenden Themen:

Forum 1	Datenschutzgerechte Chipkartensysteme
Forum 2	Verschlüsselung von Daten in der Verwaltung
Forum 3	Verläßlichkeit durch digitale Signaturen

	Forum 4	Verbesserter Patientendatenschutz durch den Computereinsatz in der Medizin?
	Forum 5	Verbraucherschutz bei Multimedia
16.00 - 17.00	Abschluß mit Berichten aus den Foren und Schlußworten	
08.00 - 18.00	Ausstellung im Foyer des Landeshauses Es werden Produkte gezeigt, die für sich in Anspruch nehmen, „im Dienste der Grundrechte“ zu wirken.	

Referenten und Podiumsteilnehmer werden u.a. sein:

Wendelin Bieser; John Borking; Prof. Dr. Hans Peter Bull, Prof. Dr. Alfred Büllesbach; Rüdiger Dierstein; Dr. Alexander Dix; Ute Erdsiek-Rave; Dr. Jürgen Eufinger; Dr. Johann Fichtner; Dr. Hansjürgen Garstka; Dr. Rüdiger Grimm; Heinz Heining; Dr. Ansgar Heuser; Peter Hohl; Dr. Michael Hortmann; Dr. Joachim Jacob; Hans-Ulrich Kaste; Dr. Werner Kessel; Dr. Dieter Klumpp; Prof. Dr. Gerhard Kongehl; Rainer König; Bernd Kowalski; Manfred Krause; Dr. Ing. Gert Lang-Lendorff; Prof. Dr. Bernd Lutterbeck; Hans Mohl; Prof. Dr. Günter Müller; Dr. Rainer Otte; Prof. Dr. Andreas Pfitzmann, Norbert F. Pötzl; Prof. Dr. Siegfried Pöppl; Prof. Dr. med. Otto Rienhoff; Dr. Ing. Karl Rihaczek; Peter Schaar; Prof. Dr. Werner Schneider; Dr. Hans-Herrmann Schrader; Welf Schröter; Gernot Schumann; Dr. Peter Sieber; Frank Simon; Peer Steinbrück; Bruno Struif; Dr. Marie-Theres Tinnefeld; Dr. Otto Ulrich; Prof. Dr. Albert von Mutius; Dr. Stefan Walz; Dr. Thilo Weichert; Meike Wolff; Dr. Theo Wolsing; Dr. Helmut Bäumler

INFORMATION UND ANMELDUNG BEIM
Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1200, Telefax: 0431/988-1223

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

Düsternbrooker Weg 82,. 24105 Kiel
Telefon: 0431/988-1200, Telefax: 0431/988-1223
E-Mail: ldsh@netzservice.de

Der Landesbeauftragte für den Datenschutz:	**Dr. Helmut Bäumler**
Dienstzimmer:	24105 Kiel, Düsternbrooker Weg 82
Dienstanschluß:	0431/988-1200
Vorzimmer:	Monika Harks App. 1202
Stellvertreter des Landesbeauftragten für den Datenschutz:	**Eckhard Beilecke** App. 1205

Referat LD 1
Dr. Helmut Bäumler
App. 1200

Silke Molt App. 1203	Grundsatzfragen des Datenschutzes Vorbereitung der Sitzung der Konferenz der Datenschutzbeauftragten Haushalt, Beschaffung, Allgemeine Verwaltungsangelegenheiten der Dienststelle Personalangelegenheiten Betreuung der DATENSCHUTZAKADEMIE
Monika Harks App. 1202	Öffentlichkeitsarbeit, Vorbereitung von Veranstaltungen, Vorbereitung von Publikationen Fortbildung
Dr. Folker Westphal App. 1208	Registratur Beschaffung von Büromaterial Haushaltsüberwachung Zusammenstellung von Arbeitsmaterial und Seminarunterlagen für die DATENSCHUTZAKADEMIE Mitarbeit bei der Führung und Veröffentlichung des Dateienregisters
Heike Reimann App. 1209 Katrin Caspari App. 1210	Sekretariat

Referat LD 2 **Eckhard Beilecke** App. 1205	
Jürgen von der Ohe App. 1206	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Kataster-, Ausländer-, Kommunal-, Gewerbe-, Bau- und Wirtschaftswesen
Holger Brocks App. 1207	Datenschutz im Bereich der Parlamentsverwaltung 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
Referat LD 3 **Uwe Jürgens** App. 1211	
Heiko Behrendt App. 1212	Datenschutz im Bereich der Steuerverwaltung 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 EDV-Einsatz der Dienststelle
Referat LD 31 **Marit Köhntopp** App. 1214	
Jan Ziegler App. 1213	Neue Medien und Informationstechniken, Medienrecht Technikfolgenabschätzung Führung und Veröffentlichung der Dateienübersicht (§ 24 LDSG)
Referat LD 4 **Herbert Neumann** App. 1215	Datenschutz im Justizbereich (ohne Staatsanwaltschaften)
Gabriele Meyer-Bettyn App. 1216	Datenschutz im Sozial- und medizinischen Bereich
Referat LD 5 **Dr. Susanne Rublack** App. 1204	Internationales Datenschutzrecht
Hans-Jürgen Strasdat App. 1217	Datenschutz im Polizei- und Verfassungsschutzbereich Datenschutz im Bereich der Staatsanwaltschaften

Beim **Landesbeauftragten für den Datenschutz** erhältliche Publikationen

Datenschutz in Schleswig-Holstein
Text des Landesdatenschutzgesetzes, der Datenschutzordnung 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 1996

Datenschutz auf Diskette
Der Landesbeauftragte für den Datenschutz hat eine Diskette herausgebracht, auf der die letzten drei Tätigkeitsberichte, die Texte des Landesdatenschutzgesetzes und der Datenschutzverordnung sowie das Programm der DATENSCHUTZ-AKADEMIE gespeichert sind. Die Diskette kann beim Landesbeauftragten kostenlos angefordert werden. Das Programm ist benutzungsfreundlich gestaltet und leicht zu bedienen. Es erlaubt den beliebigen Wechsel zwischen Tätigkeitsberichten, Texten zitierter Paragraphen des Landesdatenschutzgesetzes oder der Datenschutzverordnung und dem Programm einschlägiger Kurse der DATENSCHUTZAKADEMIE. Als Systemvoraussetzung sind ein PC 386/486 oder höher, mindestens 4 MB Hauptspeicher, MS-DOS 5.0 aufwärts und Windows 3.1 bzw. Windows für Workgroups erforderlich.

Schleswig-holsteinische Datenschutzinformationen im Internet
Auch der Landesbeauftragte für den Datenschutz nutzt moderne Kommunikationstechnologien, um Informationen zu präsentieren. Seit kurzem sind Datenschutzinformationen aus Schleswig-Holstein im weltweiten Datennetz Internet zugänglich: **http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/** (Sammlung verschiedener Datenschutzinformationen des Fachbereichs Rechtswissenschaft der Humboldt-Universität Berlin). Zur Zeit sind das Landesdatenschutzgesetz und die Datenschutzverordnung, das Programm der DATENSCHUTZAKADEMIE und die Tätigkeitsberichte der letzten Jahre im elektronischen Format abrufbar. Weitere Informationen werden folgen.