SCHLESWIG-HOLSTEINISCHER LANDTAG
14. Wahlperiode

Drucksache 14/1340
18. 03. 98

Bericht

**des Landesbeauftragten für den Datenschutz
bei dem Präsidenten des Schleswig-Holsteinischen Landtages**

**Zwanzigster Tätigkeitsbericht
(Berichtszeitraum: 1997; Redaktionsschluß: 31.1.1998)**

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

Dr. Helmut Bäumler

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

Inhaltsverzeichnis **Seite**

1.	**Zur Situation des Datenschutzes in Schleswig-Holstein**	**6**
1.1	Datenschutz im Wandel	6
1.2	Ergebnisse der Kontrollen	10
1.3	Dateienübersicht veröffentlicht	13
1.4	Die Ausstattung der Dienststelle	14
2.	**Der Weg in die Computergesellschaft**	**15**
2.1	Schleswig-Holstein als Modellregion – wofür?	15
2.2	Orwell steht wieder auf der Tagesordnung	17
3.	**Datenschutz im Landtag**	**21**
3.1	Vorschlag zur Verfassungsergänzung	21
3.2	Informations- und Kommunikationsnetz im Landtag	22
4.	**Datenschutz in der Verwaltung**	**23**
4.1	Kommunalbereich	23
4.1.1	Modellprojekt Bürgerbüro	23
4.1.2	Bauleitplanung und Öffentlichkeit von Einwendungen	24
4.1.3	Der Umgang der Mandatsträger mit Sitzungsunterlagen	26
4.1.4	Wenn Detektive Ordnungswidrigkeiten ermitteln	27
4.1.5	Grenzen für den Vollstreckungsbeamten	27
4.2	Polizei	28
4.2.1	Staatsschutz macht „klar Schiff“	28
4.2.2	Ein Bürger, das Bundeskriminalamt, INTERPOL und die kanadische Polizei	30
4.2.3	Immunität für EUROPOL-Mitarbeiter?	31
4.2.4	Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS	32
4.2.5	Schleierfahndung	33
4.2.6	Mit Videoüberwachung gegen Punker	36
4.2.7	Videoeinsatz im Strafverfahren	37
4.2.8	Privat-Fahndung im Internet	38
4.2.9	Verkehrstätigkeitsbücher	40
4.2.10	Polizei in einigen Bereichen vorbildlich	41
4.3	Verfassungsschutz	42
4.3.1	Beobachtung von Sekten?	42
4.3.2	Sicherheitsüberprüfungsgesetz längst überfällig	42
4.4	Justizverwaltung	44
4.4.1	MEGA/MESTA	44
4.4.2	Informationsfluß beim Täter-Opfer-Ausgleich	46
4.4.3	Umfang beglaubigter Ausfertigungen von Scheidungsurteilen	48

4.5	Umweltschutz	48
	Wenn ein Klimaschutzfonds die Atmosphäre verdirbt	48
4.6	Wirtschaft, Technik und Verkehr	49
4.6.1	Strafurteile in der Führerscheinakte	49
4.6.2	Zu lange Aufbewahrung von Bußgeldakten	50
4.6.3	Werbung für Radarwarngeräte – alles nur Zufall?	51
4.7	Sozialwesen	52
4.7.1	Laxer Umgang eines Vermieters mit Sozialdaten	52
4.7.2	Wenn das Sozialamt eine Blankovollmacht will	53
4.7.3	Akten von Hilfeempfängern dürfen nicht automatisch „mit umziehen“	53
4.7.4	Keine Sozialdaten für den Amtsausschuß	54
4.8	Gesundheitswesen	55
4.8.1	Computermedizin und Patientengeheimnis	55
4.8.2	„Gegendarstellung“ in der psychiatrischen Krankenakte	57
4.8.3	Datenschutz bei der Schwangerschaftskonfliktberatung	58
4.9	Kultusbereich	59
4.9.1	Wenn vertrauliche Papiere bei der Zeitung statt im Reißwolf landen	59
4.9.2	Der kurze Draht zwischen Kindergarten und Schule	59
4.9.3	Ewiger Zankapfel: Unterrichtung der Elternvertreter	61
4.10	Steuerverwaltung	62
4.10.1	Wahrung des Steuergeheimnisses im Gemeinschaftsrechenzentrum	62
4.10.2	Kontopfändung beim Herrn Bankdirektor	63
4.10.3.	Unmut über die Nutzung von Grundsteuerdaten für andere Zwecke	64
4.10.4	Kritik am Datenaustausch zwischen den Finanzämtern und den Kammern	65
4.11	Personalwesen	66
4.11.1	Wenn die Gehaltspfändung beim Fachvorgesetzten landet	66
4.11.2	Was der Amtsarzt dem Dienstherrn mitteilen darf	67
4.11.3	Neuorganisation beim polizeiärztlichen Dienst notwendig	69
4.11.4	Akteneinsichtsrecht des Personalrats	71
4.12	Angekündigte unangekündigte Kontrollen	72
5.	**Datenschutz bei den Gerichten**	**74**
5.1	Videoüberwachung im Sozialgericht	74
5.2	Gerichtsaushänge in Verfahren auf Abgabe der eidesstattlichen Versicherung	75

6.	**Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung**	**76**
6.1	30 Jahre EDV in der Verwaltung – und kein bißchen weise?	76
6.2	Automationskommission der kommunalen Landesverbände – gute Vorsätze drohen zu verwässern	78
6.3	PERMIS – wie die Technik den Weg diktiert	79
6.4	Datenschutzrechtliche Einordnung von Telearbeit	81
6.5	Wenn externe Berater das Konzept für das IT-System machen	83
6.6	Wird der Siegeszug der Informationstechnik zu einem Waterloo für die Revisionsfähigkeit der Verwaltungsabläufe?	84
6.7	Kontrollen im Bereich der automatisierten Datenverarbeitung	86
6.7.1	Zögerliche Behebung von Sicherheitsmängeln in einem Kreiskrankenhaus	86
6.7.2	Tja, wenn's ums Geld geht	87
6.7.3	Wenn die automatisierte Datenverarbeitung wirklich Chefsache ist	89
6.7.4	Der Inhalt eines typischen Prüfberichts	90
6.7.5	Wer überwacht die Fernwartung?	92
6.7.6	Noch immer nicht alle Sicherheitsprobleme im IKONET/Campus-Netz gelöst	94
6.7.7	Nachbesserungen im Schleswig-Holstein-Netz – „nur auf freiwilliger Basis"?	96
7.	**Neue Medien und Informationstechniken**	**98**
7.1	Vorbildliche Regelung des Datenschutzes bei Multimedia	98
7.2	Signaturgesetz und -verordnung	100
7.3	Verschlüsselung – ein Schlüssel zum Datenschutz	102
7.3.1	Hände weg von der Kryptographie	102
7.3.2	Verschlüsselung von E-Mail an den Datenschutzbeauftragten	105
7.4	Problematische neue Abhörbestimmungen	106
7.4.1	Beihilfe zum Abhören	106
7.4.2	Späte Erkenntnis des Gesetzgebers	107
7.4.3	Risiken der Mobiltelefonie: Handys als Peilsender und falsche Basisstationen	109
7.5	Wenn Behörden ins Internet gehen	110
7.5.1	Sicherheitskonzept und Firewall	110
7.5.2	Spezielle gesetzliche Rahmenbedingungen	111
7.6	GeldKarten mit Datenspur	112
8.	**Europa**	**114**
	Rechtzeitige Umsetzung der europäischen Datenschutzrichtlinie in Gefahr	114
9.	**Was es sonst noch zu berichten gibt**	**117**
9.1	Europäische ISDN-Richtlinie	117
9.2	Wer Forderungen gestundet haben will, muß seine Finanzlage offenlegen – aber wie detailliert?	117
9.3	Garagenplätze für Frauen scheitern nicht am Datenschutz	117
9.4	Auftragsvergabe und Frauenquote	118

9.5	Akteneinsicht: Mit gutem Willen auch komplizierte Fälle lösbar	118
9.6	Zweckbindung von Daten bei Überweisungen	118
9.7	Übergang der Personalverwaltung auf eine Privatfirma	119
9.8	Retourkutsche auf eine Beschwerde	119
9.9	Die Gefängnisverwaltungen dürfen Frauen, die sich vor der Gewalttätigkeit ihrer einsitzenden Lebenspartner fürchten, „vorwarnen“	119
9.10	Keine Blankovollmachten bei den Sozialgerichten	120
9.11	Akteneinsicht verweigert: Datenschutz gründlich mißverstanden	120
9.12	EIS-Modul nicht gesetzeskonform	120
9.13	Telefongespräche Gefangener	121
9.14	Wenn der Vollzugsabteilungsleiter mal eben mit dem Hotel telefoniert	121
10.	**Rückblick**	**122**
10.1	Videoüberwachung im Straßenverkehr	122
10.2	Neue polizeiliche Vernehmungs- und Anhörungsvordrucke	122
10.3	Verarbeitung von Versichertendaten im Auftrag (Prüfung IKK)	122
10.4	Weitergabe eines Strafurteils entgegen den Bestimmungen des Bundeszentralregistergesetzes	123
10.5	Nicht nur unzulässige CD-Roms mit Telefondaten	123
10.6	Neue Gaststättenverordnung bringt endlich Klarheit in das Konzessionsverfahren	123
10.7	Krankenscheine für Sozialhilfeempfänger neu gestaltet	124
11.	**Einige Beispiele, was durch unsere Tätigkeit besser geworden ist**	**125**
12.	**DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN**	**128**
13.	**Sommerakademie 1998**	**130**

1. Zur Situation des Datenschutzes in Schleswig-Holstein

1.1 Datenschutz im Wandel

1998 jährt sich zum 20. Mal das Inkrafttreten des ersten schleswig-holsteinischen Landesdatenschutzgesetzes. Ebensolange besteht die Dienststelle des Landesbeauftragten für den Datenschutz. Dies wäre sicher **Anlaß für Rückblicke**, Bilanzen, Anekdoten, Stolz über das Erreichte und Hader mit den Mißerfolgen sowie für Lob und Anerkennung an die Adresse der Mitarbeiterinnen und Mitarbeiter, die über all die Jahre mit viel Engagement für die Sache des Grundrechtsschutzes der Bürgerinnen und Bürger gefochten haben.

Indes, der Blick zurück kann auf einem so dynamischen Feld wie dem Datenschutz nur von kurzer Dauer sein. Nichts charakterisiert dieses Thema besser als der Blick nach vorne, die Vorbereitung auf die Aufgaben von morgen. Die vielbeschworene Informationsgesellschaft wirft ihre Schatten voraus. Überall spüren wir den **Wind der Veränderung** und den Willen der Politik, nur nichts zu versäumen und auf jeden Fall ganz vorne dabeizusein. Wie immer diese Informationsgesellschaft von morgen aussehen mag, eines ist gewiß: Ohne einen funktionierenden Datenschutz und ohne eine ausreichende Datensicherheit wird sie im Chaos enden. Nicht, daß sie technisch nicht funktionieren könnte. Aber die Menschen werden den Weg in die Informationsgesellschaft nicht mitgehen, wenn sie dies mit dem Verlust ihrer Privatsphäre und dem Abbau ihrer Grundrechte bezahlen müssen.

Deshalb warten auf den Datenschutz in den kommenden Jahren schwierige Aufgaben. Sich rechtzeitig darauf einzustellen, ist wichtiger als ein selbstgefälliger Rückblick auf das Erreichte. Noch ist kein schlüssiges Konzept für den Datenschutz im kommenden Jahrzehnt entwickelt. Analysiert man aber die Fakten, wird in Umrissen erkennbar, welche Veränderungen zwangsläufig vorgenommen werden müssen:

- **Eine neue Rezeption des Volkszählungsurteils!**

Das Volkszählungsurteil von 1983 war einer der wichtigsten „Erfolge", die der Datenschutz in den vergangenen beiden Jahrzehnten errungen hat. Es hat ihn mit Verfassungsrang in der Staatspraxis etabliert und allen Auffassungen, es handle sich um eine vorübergehende Modeerscheinung, eine klare Absage erteilt. Allerdings haben sich nicht alle Erwartungen erfüllt, die das Urteil geweckt hat. Datenschutzbeauftragte und Bürger mußten die Erfahrung machen, daß **immer mehr gesetzliche** Vorschriften nicht automatisch auch mehr Datenschutz bedeuten. Das grundlegende Mißverständnis, dem Bundesverfassungsgericht sei es in erster Linie um die Schaffung neuer gesetzlicher Grundlagen gegangen, führte zu einer Gesetzeslawine ohnegleichen. Da die dem Gesetzgeber obliegende Prüfungsfrage, ob den Bürgern die betreffenden Daten überhaupt abverlangt werden müssen, von der Verwaltung stets umgehend mit „Ja" beantwortet und auf Wunsch auch wort-

reich begründet wurde, folgten Jahre nach dem Motto: Man darf im Prinzip „alles", man muß nur eine gesetzliche Grundlage schaffen. Auf diesem Weg sind eine Reihe von Normen entstanden, auf denen zwar außen „Datenschutz" draufsteht, in denen aber kein oder nur wenig Datenschutz drin ist. Gesetze, die von dem Ehrgeiz beseelt sind, für alle denkbaren Verarbeitungs- und Nutzungsvarianten vorsorglich Rechtsgrundlagen zu schaffen, enthalten eine Fülle von Sonder-, Ausnahme- und Ausnahme-von-der-Ausnahmetatbeständen, sind nur schwer lesbar und alles andere als **normenklar**. Sie frustrieren die Behörden, weil das, was sie glauben ohnehin tun zu müssen, nunmehr in komplizierten Vorschriften detailliert geregelt ist, und sie führen zur Resignation der Bürger, die die Feststellung machen müssen, daß solche Gesetze zwar vermeintlich umfängliche „Datenschutzbestimmungen" enthalten, im Kern aber nur das Handeln der Behörden formalrechtlich perfekt absichern.

Für die Zukunft ist daraus der Schluß zu ziehen, daß die Schaffung von Rechtsgrundlagen die Position der Bürger nicht per se verbessert. Die Grundsätze der **Datenvermeidung** und **Datensparsamkeit** müssen von Gesetzgeber und Verwaltung ernster als bisher genommen werden. Nicht jedes Detail muß gesetzlich geregelt werden. In Bereichen, die nicht so sensibel wie z. B. der Gesundheits-, Sozial- oder Sicherheitsbereich sind, muß ein gesunder Mix von fairen Generalklauseln und Spezialvorschriften angestrebt werden. Das Datenschutzrecht darf seinen Vertrauensbonus nicht durch einen Etikettenschwindel verlieren, der aus Schutzbestimmungen Eingriffsermächtigungen macht.

- **Neue Prioritäten setzen!**

Die Datenschutzbeauftragten müssen sich bei ihrer Tätigkeit stärker auf die wirklich wichtigen Probleme konzentrieren. Sonst entsteht die Gefahr der **Bürokratisierung** und **Zerfaserung** ihres Handelns mit manchmal skurrilen Ergebnissen. Bezeichnenderweise werden sie zu verqueren Randfragen oft und gerne von denjenigen als Schiedsrichter angerufen, die im übrigen mit dem Datenschutz nicht allzuviel im Sinn haben. Beamte, die bei ihrer Tätigkeit mit dem Datenschutz der Bürger eher lax umgehen, rufen dann den Datenschutzbeauftragten an, wenn es um die Frage geht, ob ihr Name auf dem Türschild ihres Dienstraumes oder im Geschäftsverteilungsplan erscheinen darf. Auch in anderen Bereichen finden sich merkwürdige Ungereimtheiten. Die Datenschutzbeauftragten beklagen beispielsweise seit Jahren vergeblich, daß die Prozeßordnungen kaum Datenschutzbestimmungen enthalten, so daß selbst sensibelste Prozeßakten nur unzulänglich vor Mißbrauch geschützt sind. Auf der anderen Seite fragen immer wieder ernsthaft einzelne Richter nach, ob ihre Pflicht, die Urteile namentlich zu unterzeichnen, nicht gegen den Datenschutz verstößt.

Die Verzettelung und Marginalisierung kann vermieden und die **Konzentration** auf die **zentralen Anliegen** des Datenschutzes kann erleichtert werden, wenn ein wichtiger Satz des Volkszählungsurteils in Zukunft stärker beachtet wird. Zwar hat das Gericht zu Recht betont, daß es kein von vornherein belangloses Datum gibt, aber hinzugefügt, daß es entscheidend auf den Verwendungszusammenhang

ankommt. Die Verwendungszusammenhänge transparent zu machen und zu bewerten, wird künftig für die Datenschutzbeauftragten eine der Aufgabenstellungen mit höchster Priorität sein.

- **Die Technik zum Verbündeten machen!**

Bei vielen Betrachtern hat der Datenschutz bisher offenbar den Eindruck erweckt, letztlich sei er ein Instrument zur Technikverhinderung; immerhin betonen einige Passagen des Volkszählungsurteils die besonderen Risiken der automatisierten Datenverarbeitung ausdrücklich. Richtig daran ist, daß aus den Möglichkeiten der Datenverarbeitungstechnik große und **neuartige Risiken** für das Persönlichkeitsrecht und die Privatsphäre entstehen. Andererseits erwachsen aus der Technik auch mehr und mehr Instrumente für einen wirksameren Schutz der genannten Rechtsgüter, als es in der Vergangenheit möglich war.

Datenvermeidung, Anonymisierung, Pseudonymisierung und Verschlüsselung sind nur einige Beispiele dafür, welch mächtigen Verbündeten die Privatsphäre in der Technik haben kann. Die Aufgabe der Datenschutzbeauftragten wird in den kommenden Jahren sein, den Aspekt „**Datenschutz durch Technik**" zu einem zentralen Ansatz zu machen. Sie werden dabei, nicht nur bei den Bürgern, sondern – das ist allerdings neu – insbesondere bei den Technikern auf Verbündete treffen. Die in Deutschland gerade beginnende Diskussion über den Erhalt der Freiheit, Daten nach Belieben zu verschlüsseln, vermittelt einen ersten Eindruck davon, welche bisher nicht für möglich gehaltenen Allianzen zwischen Datenschutz, Herstellern, Wirtschaft und Informatik sich entwickeln werden.

- **Den größeren Zusammenhang sehen!**

Den Datenschutz als eindimensionales, isoliertes Abwehrrecht zu betrachten, greift zu kurz. Statt dessen muß er als Teil einer sich langsam aber kontinuierlich entwickelnden, umfassenden neuen Informationsordnung begriffen und praktiziert werden. Die Technik setzt dabei die Rahmenbedingungen. Die klassischen Trennlinien zwischen isolierter Datenverarbeitung, Telekommunikation und Medien verschwinden immer mehr und machen Platz für eine umfassende **Konvergenz** der Systeme. Hierauf muß auch der Datenschutz Bezug nehmen. Zu berücksichtigen ist aber auch folgendes: Auf Dauer werden die Bürger ein allgemeines **Zugangsrecht** zu staatlichen **Informationen** und womöglich auch zu Informationen großer privater Wirtschaftsunternehmen durchsetzen. Soeben hat die Europäische Union in Artikel 255 des Vertrages von Amsterdam einen Meilenstein auf dem Weg dorthin gesetzt und den Zugang zu den Dokumenten des Europäischen Parlamentes, des Rates und der Kommission für jedermann eröffnet. Es ist nur eine Frage der Zeit, bis auch die Parlamente in Deutschland auf breiter Front den allgemeinen Informationszugang beschließen werden. Dem Datenschutz kommt bei diesem Vorgang nicht die Bremserrolle zu, sondern die Aufgabe, einen abgewogenen Ausgleich zwischen dem Recht auf Informationszugang und der Pflicht zur Beachtung der grundrechtlichen Belange derjenigen herzustellen, deren perso-

nenbezogene Daten auf diese Weise gegebenenfalls in die Öffentlichkeit gelangen könnten.

- **Serviceorientierung ist gefragt!**

Daß die Datenschutzbeauftragten in der Vergangenheit mit ihren Kontrollen wesentliche Rechtsverstöße aufgedeckt und beseitigt haben, ist unter Fachleuten unbestritten. Der breiten Öffentlichkeit ist aber nicht bewußt geworden, daß die Republik ein anderes Aussehen hätte, wenn es in den vergangenen zwanzig Jahren keine Datenschutzkontrollen gegeben hätte. Auch in Zukunft sind deshalb **effektive Kontrollen unverzichtbar**. Wenn der Staat seine Datenerhebung zum Beispiel im Sicherheitsbereich immer mehr mit heimlichen Methoden betreibt, müssen sich die Bürgerinnen und Bürger darauf verlassen können, daß diese für sie undurchschaubare Datenverarbeitung wirksam kontrolliert wird.

In offenen Netzen wie dem Internet versagen aber traditionelle staatliche Kontrollmethoden. Diese Erfahrung müssen gerade naßforsche Staatsanwälte machen, die das Internet mit herkömmlichen Mitteln „sauberhalten" wollen. Auch die Datenschutzbeauftragten können den Datenschutz der Bürger im Internet mit ihren bisherigen Kontrollmethoden nicht mehr garantieren. Die Betroffenen können sich aber selbst wirksam und effektiv schützen, z. B. durch Verschlüsselung. Hierbei brauchen sie die Unterstützung durch fachkundige Berater. Darauf müssen sich die Datenschutzbeauftragten rechtzeitig einstellen. Neben der traditionellen Kontrolle wird der **Service** der **Datenschutzbeauftragten** als **„Kompetenzcenter"** in allen Fragen des Datenschutzes und der Datensicherheit eine immer größere Bedeutung erhalten. Auch gegenüber den Behörden sind nicht nur Überzeugungsarbeit und unzweideutige Kritik bei Rechtsverstößen, sondern ebensosehr die Unterbreitung brauchbarer, überzeugender Handlungskonzepte gefragt.

- **Konzentration der Kräfte!**

Last but not least wird es höchste Zeit, daß die Kräfte und Mittel der Datenschutzkontrolle konzentriert und durch Gewinnung von **Synergieeffekten** optimiert werden. Es ist kaum jemandem zu vermitteln, daß in vielen Ländern, so auch in Schleswig-Holstein, die ohnehin geringen personellen und sachlichen Ressourcen für den Datenschutz noch einmal zwischen der Kontrolle über den öffentlichen und die Aufsicht über den privaten Bereich aufgespalten werden. Bürger, die sich an uns wenden, haben kein Verständnis dafür, wenn wir sie nach Erläuterung der komplizierten Zuständigkeitsregeln an die Aufsichtsbehörde verweisen müssen. Die dortigen Kollegen machen die gleichen Erfahrungen. Aus der Sicht der Bürger ist diese Zersplitterung der Zuständigkeiten das Gegenteil von Bürgerservice, Kundenorientierung und Effektivierung der Verwaltung.

Die Modernisierung der öffentlichen Verwaltung ist mit einer zunehmenden Verwischung der Grenzen von öffentlichem Recht und Privatrecht verbunden. Es kann nicht sein, daß die Datenschutzkontrolle je nach gewählter Rechtskonstruktion zwischen Datenschutzbeauftragten und Aufsichtsbehörden hin und her

pendelt. So ist z. B. untragbar, daß Kliniken, solange sie in öffentlicher Trägerschaft sind, unserer Kontrolle, sobald sie privatisiert werden, der Kontrolle durch den Innenminister unterliegen. Sicher, wir stimmen unsere Positionen auf diesem schwierigen Feld mit hohem Aufwand ab. Ganz ausschließen kann man allerdings nicht, daß beim gleichen Problem **mit zweierlei Maß gemessen** wird, nur weil die Rechtsform der Trägerschaft unterschiedlich ist. Die Patienten müssen sich aber darauf verlassen können, daß die Beachtung des Arztgeheimnisses stets in gleicher Weise gewährleistet ist, egal ob sie sich in eine Privatklinik oder in ein kommunales Krankenhaus begeben.

Die Datenschutzkontrolle ist in Deutschland personell und sachlich so kümmerlich ausgestattet, daß die Zersplitterung der Kräfte ein unhaltbarer Anachronismus ist. Den **Luxus von Minibehörden**, die bei faktisch gleicher Aufgabenstellung nebeneinanderherarbeiten, können wir uns in der gesamten staatlichen Verwaltung nicht länger leisten, schon gar nicht bei der Datenschutzkontrolle. Die Aufgaben der Zukunft können nur mit einer Konzentration der Kräfte gemeistert werden. Deshalb sollten die Kontrolle über den öffentlichen Bereich und die Aufsicht über den Privatbereich so schnell wie möglich zusammengelegt und als völlig unabhängige Kontrollbehörde ausgestaltet werden, so wie das die Datenschutzrichtlinie der Europäischen Union vorschreibt. Darüber hinaus müssen neue Formen der Kooperation zwischen den Kontrollbehörden der Bundesländer sowie im internationalen Rahmen erprobt werden. Im Zeitalter des Internets ist Kleinstaaterei auf dem Gebiet der Datenschutzkontrolle nicht mehr zeitgemäß.

1.2 Ergebnisse der Kontrollen

Wie in jedem Jahr bildeten auch 1997 die Kontrollen vor Ort das Kernstück unserer Tätigkeit. Große „Skandale" gibt es nicht zu vermelden. Neben vielen Kritikpunkten im Detail gab es sogar ausdrücklich lobenswerte Resultate (vgl. Tz. 4.8.4 und Tz. 6.7.3). Die vielen datenschutzrechtlichen **Beanstandungen der Vergangenheit** beginnen offenbar Früchte zu tragen. Die Behörden tauschen mehr und mehr unsere Prüfberichte untereinander aus und versuchen, Mängel von vornherein zu vermeiden. Auch die Kurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN zeigen Wirkung und tragen zu einem spürbar höheren Datenschutzniveau bei.

Gleichwohl gab es auch in diesem Jahr genug zu kritisieren. Häufig wird unterschätzt, daß auch vermeintlich kleine **Fehler** für den Betroffenen **spürbare Folgen** haben können. Da Datenschutz Gefahrenabwehr ist, gilt es, derartige Risikofaktoren nach Möglichkeit an der Wurzel zu bekämpfen, bevor sie Schaden verursachen. Beispiele für Mängel, die wir nach Kontrollen zu beanstanden hatten:

- zu lange Aufbewahrung von Akten über Verkehrssünder (Tz. 4.6.2),
- automatische Übersendung der kompletten Sozialhilfeakten bei jedem Wohnsitzwechsel (Tz. 4.7.3),

- routinemäßige Abforderung von Blankovollmachten von Sozialhilfeempfängern (Tz. 4.7.2),
- Vorabinformation der Psychologen bei medizinisch-psychologischen Untersuchungen ohne Kenntnis des Betroffenen (Tz. 4.6.1),
- Einsatz einer Videokamera in der Antragsstelle eines Sozialgerichts (Tz. 5.1),
- regelmäßige Unterrichtung der Fachvorgesetzten über Gehaltspfändungen (Tz. 4.11.1).

Erstmals haben wir im vergangenen Jahr mit einem neuen Prüfkonzept den sorgfältigen Umgang mit personenbezogenen Daten im Behördenalltag geprüft (Tz. 4.12). Dabei erhielten die Behörden zwar vorher eine abstrakte „Vorwarnung", die eigentliche **Prüfung** erfolgte aber **unangemeldet**. Die Prüfer gerierten sich dann wie „neugierige Besucher". Was sie dabei zu sehen bekamen, war teilweise besorgniserregend. Die Gedankenlosigkeit, mit der z. B.

- Bürotüren offenstanden, obwohl sensible Sozialdaten auf dem Tisch lagen,
- Unterlagen über ein Strafverfahren einfach in den Papierkorb auf dem offenen Flur geworfen wurden,
- Akten mit brisantem Inhalt frei zugänglich bis zur Vernichtung „zwischengelagert" wurden,

führte zu zahlreichen Beanstandungen.

Andererseits konnte man aber bei einigen Behörden auch angenehm überrascht sein, wie sorgsam die Aspekte der Datensicherheit beachtet wurden. Insgesamt sind die Ergebnisse der bisher durchgeführten „angekündigten unangekündigten Kontrollen" (sogenannte AUK) also gemischt. Wir werden die Aktion in diesem Jahr fortsetzen.

In dem Maße, in dem die **Informationstechnik** Einzug in die öffentliche Verwaltung hält, verlagert sich unsere Kontrolltätigkeit immer mehr auf die technisch-organisatorischen Aspekte. Hier lag auch im Berichtsjahr der Schwerpunkt unserer Aktivitäten. Die festgestellten **Mängel** auch bei neu eingeführten EDV-Verfahren waren teilweise **erschreckend**. Das Problematische ist, daß sie nicht immer sofort zu Schäden und Nachteilen führen. Langfristig tickt aber eine **Zeitbombe**, wenn die Automatisierung der Datenverarbeitung vor allem in kleineren und mittleren Behörden im gleichen Stil wie bisher weiterbetrieben wird. Es muß zu denken geben, daß wir – von löblichen Ausnahmen abgesehen (Tz. 6.7.2 und Tz. 6.7.3) – immer wieder die gleichen Feststellungen treffen mußten:

- fehlende Vorstellung, was eigentlich mit Hilfe des EDV-Systems erreicht werden soll,
- fehlendes Sicherheitskonzept, mit dem gewährleistet werden soll, daß nicht erwünschte Effekte auch wirksam verhindert werden,

- ungenügende Tests,
- fehlende EDV-Schulung der Mitarbeiter,
- daraus folgend die zunehmende Einschaltung unkontrollierbarer externer Dienstleistungsfirmen.

Uns beunruhigen diese Mängel insbesondere, weil niemand die Einhaltung der Datenschutzbestimmungen wirklich gewährleisten kann, wenn er sein EDV-System mangelhaft konzipiert und in der Folge dann nicht beherrscht. Nicht beherrschbare EDV-Systeme sind langfristig eine **Bedrohung** der **Revisionsfähigkeit** des Verwaltungshandelns insgesamt (Tz. 6.6). Es ist alarmierend, wenn uns gestandene Bürgermeister oder Kämmerer eingestehen, sie könnten seit Einführung ihrer neuen EDV-Verfahren nicht ruhig schlafen. Sie würden von der Sorge umgetrieben, daß sie die Verantwortung das Verwaltungshandeln ihrer Behörde nicht wie bisher übernehmen könnten.

Dabei ist eine ordnungsgemäße, sichere Datenverarbeitung durchaus keine Hexerei. Auch wenn es gar kein Datenschutzrecht gäbe, leuchtet ein, daß die Einführung neuer EDV-Verfahren nach folgenden Gesichtspunkten abgewickelt werden muß:

- Es muß klar sein, daß **automatisierte Verwaltungsabläufe** sich nicht im Einsatz von Computern erschöpfen, sondern ein Zusammenspiel von Hardware, Software, Datenbeständen sowie Aufbau- und Ablauforganisation sind. Wird eine Komponente vernachlässigt, werden alle anderen in Mitleidenschaft gezogen.
- Wer ein IT-System plant, muß am Ende der Planungsphase wissen, was er will. Schreibt er diese Absichten auf, hat er ein nachvollziehbares **IT-Konzept**. Dies darf kein Feigenblatt, sondern muß die Bauzeichnung sein, nach der das System aufgebaut wird.
- Auf dieser Grundlage läßt sich dann das **Sicherheitskonzept** erstellen, in dem beschrieben wird, wie erreicht werden soll, daß das IT-System (nur) so funktioniert, wie es im IT-Konzept und in den gesetzlichen Bestimmungen festgelegt ist. Dabei sind nicht akademische Abhandlungen gefragt, sondern konkrete Handlungsanweisungen zur Abwehr konkreter Risiken in einer konkreten Behörden.
- Vor dem Echtbetrieb sind **Tests** durchzuführen. Da vor allem kleinere und mittlere Behörden derartige Tests nicht selbst durchführen können, müssen Wege der Kooperation gefunden werden. Hier sind vor allem die kommunalen Landesverbände gefordert.
- Alle Komponenten des IT-Systems sowie alle Aktivitäten zur Durchführung von Veränderungen sind so zu **dokumentieren**, daß sie für die Verantwortlichen und für sachverständige Dritte nachvollziehbar sind.
- Alle Mitarbeiter, die mit dem IT-System arbeiten oder seinen korrekten Einsatz verantworten, müssen rechtzeitig **geschult** werden.

- Sollen **externe Dienstleister** z. B. für Reparatur- und Wartungsarbeiten eingesetzt werden, müssen exakte vertragliche Regelungen getroffen werden. Dabei muß auch festgelegt sein, daß die Aktivitäten der externen Dienstleister in einer Weise zu dokumentieren sind, daß die Verwaltung auch ihnen gegenüber das Heft in der Hand behält.

Wir haben im Berichtsjahr wieder erhebliche Kapazitäten in die **Beratung** der Behörden, die ein neues IT-Verfahren planten, gesteckt. Häufig waren unsere Mitarbeiter tagelang damit beschäftigt, einer einzelnen Kommune bei der Erstellung ihrer EDV-Konzeption unter die Arme zu greifen. Dieser Einsatz zahlt sich aus. Bei EDV-Verfahren, die der Datenschutzverordnung entsprechen, sinkt das Risiko, daß es durch unsachgemäßen Technikeinsatz zu einer Verletzung der schutzwürdigen Belange der Bürgerinnen und Bürger kommt. Für die Kommunen hat unsere Beratung den angenehmen Nebeneffekt, daß sie sich entweder kostspielige Serviceleistungen von vornherein sparen können oder zigtausend Mark teure Consultinggutachten besser auf ihre Umsetzbarkeit prüfen können. So gesehen, erfüllt die Beratungstätigkeit den Servicegedanken auf zweierlei Weise: Sie nutzt dem informationellen Selbstbestimmungsrecht der Bürgerinnen und Bürger und hilft den Gemeinden, manche Mark zu sparen. Langfristig wird überdies der Kontrollbedarf gesenkt, wenn EDV-Systeme von vornherein datenschutzgerecht konzipiert werden.

1.3 Dateienübersicht veröffentlicht

Die im Mai 1997 veröffentlichte Übersicht gibt erstmals einen Überblick über die Verarbeitung personenbezogener Daten in Dateien bei den Behörden in Schleswig-Holstein. Sie beruht auf den von den öffentlichen Stellen des Landes erstellten und uns zugesandten **Dateibeschreibungen**. Bei der Novellierung des Landesdatenschutzgesetzes im Jahre 1992 wurde eine Bestimmung eingefügt, wonach alle fünf Jahre in geeigneter Weise eine Dateienübersicht zu veröffentlichen ist.

Das jetzt erstmals veröffentlichte Register bildet – obwohl keineswegs alle Behörden ihrer gesetzlichen Meldepflicht nachgekommen sind – einen eindrucksvollen Überblick über die Verarbeitung personenbezogener Daten in Schleswig-Holstein. Insgesamt sind mehr als **3 400 Dateien** von etwa **500 Behörden** erfaßt. Nicht erfaßt sind allerdings Speicherungen bei Bundesbehörden wie z. B. beim Kraftfahrt-Bundesamt oder bei den Arbeitsämtern und bei Wirtschaftsunternehmen wie Banken und Versicherungen, da diese Stellen nicht unserer Kontrolle unterliegen. Jeder Bürger kann sich leicht ausrechnen, daß er in Hunderten von Dateien registriert ist.

Bislang hat das Datenschutzrecht dafür gesorgt, daß diese vielen Daten nicht alle zusammengeführt und zu einem detaillierten **Persönlichkeitsprofil** verknüpft werden dürfen. Die Veröffentlichung versteht sich deshalb auch als Appell, trotz Verschlankung, Modernisierung und Kosteneinsparung am Prinzip der **Zweckbindung** festzuhalten und nicht den gläsernen Bürger zu schaffen. Vielmehr ist die Übersicht ein Beitrag, umgekehrt die Datenverarbeitung der Verwaltung für

den Bürger transparent zu machen. Anhand des Registers können die Bürgerinnen und Bürger prüfen, wo Daten über sie gespeichert sein könnten, um dort unter Umständen ihren Auskunftsanspruch geltend zu machen.

Die Veröffentlichung ist aber auch ein Plädoyer, das **Datenschutzgesetz weiterzuentwickeln** und den raschen Veränderungen der Informationstechnik anzupassen. Das Datenschutzrecht muß stärker als bisher **dezentrale Elemente** aufnehmen. Es versteht sich von selbst, daß wir bei unserer Personalkapazität nur einen geringen Bruchteil der Datensammlungen überprüfen können. Auch die im Register erfaßten Dateien sind überwiegend datenschutzrechtlich noch nicht geprüft. Deshalb sollte schon vor Ort durch behördliche Datenschutzbeauftragte eine Vorkontrolle gewährleistet sein. In diesem Zusammenhang könnte dann auch auf die enorm zeit- und personalintensive Registrierung der Dateien an einer zentralen Stelle verzichtet und einzelne Register bei den Behörden geführt werden. Dort sind sie nämlich auch in Zukunft unverzichtbar, um den Überblick über die bei der datenverarbeitenden Stelle vorhandenen Datensammlungen zu behalten.

1.4 Die Ausstattung der Dienststelle

In der Dienststelle sind derzeit 20 Mitarbeiterinnen und Mitarbeiter tätig. Wegen der schwierigen Haushaltssituation haben wir für 1998 keine neuen Stellen bekommen. Angesichts der ungebremsten **Dynamik der Informationstechnik**, die die Landesregierung auf allen Ebenen fördert und propagiert, können wir deshalb unsere Aufgaben nur durch Schwerpunktbildung und häufig überdurchschnittliches Engagement der Mitarbeiterinnen und Mitarbeiter erledigen.

Die Ausstattung des **IT-Labors** ist weiter verbessert worden. Wir sind zunehmend in der Lage, neue Softwareprodukte unter datenschutzrechtlichen Aspekten genau unter die Lupe zu nehmen. Durch Einrichtung eines eigenen Testnetzes können datenschutzrechtliche Schwachstellen systematisch untersucht werden. Die Ergebnisse kommen Bürgern und Behörden im Rahmen unserer Beratungstätigkeit unmittelbar zugute.

Nach wie vor tragen die Kurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN (Tz. 12) zur Effektivierung unserer Arbeit bei. Wir können auf diesem Weg für unsere Forderungen und Ratschläge einen guten **Multiplikatoreffekt** erzielen. Die Ergebnisse der Kontrollen im Berichtsjahr zeigen, daß die in den Kursen gewonnenen Erkenntnisse offenbar auch in der Praxis umgesetzt werden.

2. Der Weg in die Computergesellschaft

2.1 Schleswig-Holstein als Modellregion – wofür?

Mit Engagement und Geschick hat sich Schleswig-Holstein unter zahlreichen Mitbewerbern durchgesetzt und ist von der Europäischen Union als eine von 23 Modellregionen für den Weg in die Informationsgesellschaft ausgewählt worden. Im vergangenen Jahr wurden im Rahmen dieser „**Regional Information Society Initiative**" (RISI) zahlreiche Arbeitsgruppensitzungen durchgeführt, an denen wir uns beteiligt haben. Außerdem haben wir an einigen öffentlichen RISI-Diskussionsveranstaltungen durch Vorträge mitgewirkt.

Die Landesregierung treibt die Einführung der elektronischen Datenverarbeitung voran, wo es nur geht. Von der Aktion „Schulen ans Netz" über „Schulen ins Netz" bis hin zur Förderung der Telearbeit und zur jüngsten Initiative „Multimedia Schleswig-Holstein" unternimmt sie viele Anstrengungen, damit das Land nicht den Anschluß verpaßt. Dies tun auch die Regierungen anderer Länder. Worin soll nun das Modellhafte bestehen? Wodurch soll sich Schleswig-Holsteins Weg in die Informationsgesellschaft unverwechselbar von dem anderer Länder unterscheiden?

Eine Möglichkeit könnte sein, nicht nur eine optimale technische Ausstattung anzustreben, den Wettbewerb also ausschließlich über immer mehr EDV zu suchen. Das Land könnte sich daneben zum Ziel setzen, den Übergang in die Informationsgesellschaft möglichst so zu gestalten, daß die **grundlegenden Prinzipien** der Verfassung – zum Beispiel die freiheitliche Demokratie, die Effektivierung des Grundrechtsschutzes, der Sozialstaatsgrundsatz – gerade unter den neuen Bedingungen der Informationsgesellschaft besser als bisher verwirklicht werden. Dadurch könnte es gelingen, der Diskussion um die Informationsgesellschaft etwas von ihrem kalten, technokratischen Beigeschmack zu nehmen, der viele Menschen beunruhigt. Wir haben im Rahmen unserer Mitarbeit am RISI-Projekt insgesamt vier konkrete Vorschläge unterbreitet, die bei den Verantwortlichen ein unterschiedliches Echo gefunden haben:

- **Vorschlag zur Verfassungsergänzung**

  Unseren Vorschlag zur Ergänzung der schleswig-holsteinischen Landesverfassung um einen Artikel „**Teilhabe an der Informationsgesellschaft**" haben wir sowohl der Landesregierung als auch dem Parlament unterbreitet. Während uns von seiten der Landesregierung keine Reaktion zugegangen ist, griff die Enquete-Kommission „Verfassungsreform" den Vorschlag auf (vgl. Tz. 3.1).

- **Projektvorschlag für eine netzunterstützte Lehreinrichtung**

  Der Ministerpräsidentin haben wir vorgeschlagen, einen Lehrstuhl einzurichten, der sich systematisch mit den durch die Informationsgesellschaft entstehenden Fragen für unser demokratisches System, für die Grundrechte im allgemeinen und für Datenschutz und Datensicherheit im besonderen befassen

soll. Es sollte sich um ein **interdisziplinäres Projekt** handeln, das zumindest die Bereiche Informatik sowie Rechts- und Gesellschaftswissenschaften umfaßt. In unserem Projektvorschlag haben wir u. a. folgendes ausgeführt:

- Gerade wegen des Zerfalls traditioneller Bindungen kommt der Wahrung und Effektivierung der Grundrechte in der Informationsgesellschaft eine zentrale Integrationsfunktion zu.
- Die Informationstechnik ist gestaltungsoffen. Sie bedarf der Steuerung durch die Menschen, nur sie dürfen entscheiden, welche technischen Mittel zu welchen Zwecken eingesetzt werden.
- Es muß rechtzeitig gezielt und systematisch untersucht werden, welche Risiken für das informationelle Selbstbestimmungsrecht durch welche grundrechtsfreundlichen Techniken bekämpft werden können.
- Die Datensicherheitstechnik darf nicht nur die Bedürfnisse der Systembetreiber abdecken, sondern muß vielmehr die Sicherheit möglichst aller von einem Datenverarbeitungsverfahren Betroffenen berücksichtigen.

Nach unserer Vorstellung soll der neue Lehrstuhl diese und weitere Fragen wie eine „**Zukunftswerkstatt**" wissenschaftlich aufbereiten und Politik und Gesellschaft kontinuierlich beraten. Der Lehrstuhl sollte ein Lernnetzwerk aufbauen, das es allen Interessierten aus Wissenschaft und Gesellschaft ermöglicht, am Diskurs teilzuhaben. Er sollte deshalb sein Lehr- und Diskussionsangebot auch „**virtuell**", d. h. über das Netz, zur Verfügung stellen und so den Kreis der üblichen akademischen Diskussion erweitern.

Die Ministerpräsidentin bedankte sich für den Vorschlag und leitete ihn an das Wissenschaftsministerium weiter. Dort fand vor Monaten ein Gespräch ohne greifbares Ergebnis statt. Seitdem haben wir von der Angelegenheit nichts mehr gehört.

- **Vorschlag zur Einrichtung eines Anonymous-Servers**

Die neuen Multimediagesetze sehen vor, daß die Nutzer auch anonym oder unter Pseudonym auf Informationsangebote zugreifen können, wenn dies „**technisch möglich und zumutbar**" ist (vgl. Tz. 7.1). Die theoretischen Fragen im Zusammenhang mit der Einrichtung von Servern, die den anonymen Zugang garantieren, sind seit Jahren weitgehend geklärt. Jetzt kommt es darauf an, solche Systeme tatsächlich zu installieren und praktisch zu erproben. Wir haben deshalb der Technologiestiftung vorgeschlagen, ein Gemeinschaftsprojekt zwischen der Technischen Universität Dresden, einigen mittelständischen Providern aus Schleswig-Holstein und unserer Dienststelle durchzuführen. Damit sollen Zugänge, z. B. zur Drogenberatung, über das Internet angeboten und den Nutzern Anonymität garantiert werden. Bei Redaktionsschluß des Berichts lag die Antwort der Technologiestiftung noch nicht vor.

- **Modernisierung der Arbeit der Datenschutzbeauftragten**

Wir haben damit begonnen, für unsere eigene Arbeit schon frühzeitig die Weichen für die kommenden Herausforderungen der Informationsgesellschaft zu stellen. Für die Sommerakademie 1998 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN lautet das Thema deshalb: „Datenschutz in der Informationsgesellschaft von morgen" (vgl. Tz. 13). Juristen, Informatiker, Hersteller, Anbieter, Politiker, Bürgerinnen und Bürger und Datenschützer werden sich mit neuen Ideen und Ansätzen für die Datenschutzkontrolle in den kommenden Jahren befassen. Die Veranstaltung wird mit Unterstützung der Technologiestiftung durchgeführt.

2.2 Orwell steht wieder auf der Tagesordnung

Im Jahre 1970 hatte das Bundesverfassungsgericht über die im Zuge der Notstandsgesetze neu eingeführten Bestimmungen zum Abhören von Telefonen zu entscheiden. Mit der knappen Mehrheit von nur einer Stimme ließ das Gericht damals die Gesetze passieren. In der Begründung der unterlegenen Richter findet sich folgender Satz: „... *ob der mit der Verfassungsänderung vollzogene erste Schritt auf dem bequemen Weg der Lockerung der bestehenden Bindungen nicht Folgen nach sich zieht, vermag niemand vorherzusehen.*" Rückblickend zeigt sich tatsächlich, daß, nachdem der Damm einmal gebrochen war, die **staatlichen Abhörmöglichkeiten** kontinuierlich erweitert und von Jahr zu Jahr stärker in Anspruch genommen wurden. Hier die Fakten:

- Seit dem Urteil ist der **Katalog** der **Straftaten,** bei deren Aufklärung Telefone abgehört werden dürfen, 16mal erweitert worden und umfaßt jetzt über 20 neue Tatbestände gegenüber der Ursprungsfassung.

- Von 1990 bis 1996 stieg die Zahl der Anordnungen, Telefonanschlüsse abzuhören, von 2 494 auf 6 428. Von diesen **Abhörmaßnahmen** sind tausende von Menschen betroffen, die Telefongespräche über die abgehörten Anschlüsse geführt haben. Allein in einem Fall wurden z. B. über 120 000 Telefongespräche auf der Grundlage einer einzigen Anordnung abgehört.

- 1992 erhielt die Polizei zur Bekämpfung der **Organisierten Kriminalität** erstmals die Befugnis, nichtöffentliche Gespräche außerhalb von Wohnungen abzuhören und aufzuzeichnen.

- 1994 wurde der **Bundesnachrichtendienst** ermächtigt, zur Bekämpfung der Organisierten Kriminalität den internationalen Fernmeldeverkehr über Funkstrecken (also die Mehrzahl der grenzüberschreitenden Telefonate) vollständig und ohne konkreten Strafverdacht abzuhören sowie nach bestimmten Suchbegriffen auszuwerten.

- Seit der **Digitalisierung** des Telefonverkehrs in den letzten Jahren können die nunmehr vollständig aufgezeichneten **Verbindungsdaten** auf der Grundlage des Fernmeldeanlagengesetzes „in strafgerichtlichen Verfahren" verwendet werden.

- 1996 verpflichtete das **Telekommunikationsgesetz** die privaten Telekommunikationsanbieter, den Sicherheitsbehörden (also auch den Geheimdiensten) einen Online-Zugriff auf die Kundendaten zu eröffnen. Er muß so gestaltet sein, daß die Anbieter den Datenabruf durch die Sicherheitsbehörden nicht bemerken können.

- Durch das **Telekommunikations-Begleitgesetz von 1997** wurden die privaten Telekommunikationsanbieter auch verpflichtet, den Sicherheitsbehörden das Abhören von Telefongesprächen zu ermöglichen. Sie haben außerdem folgende **Verbindungs- und Bestandsdaten** zur Verfügung zu stellen, wenn eine richterliche Abhörgenehmigung vorliegt:

  - Die vom überwachten Anschluß angewählten Rufnummern und Zusatzdienste sowie die Nummern der Anschlüsse, die den überwachten Anschluß angewählt haben, auch wenn keine Verbindung zustande kommt,
  - Rufumleitungen oder -weiterschaltungen,
  - bei überwachten Mobilanschlüssen die Funkzellen, über die die Verbindung abgewickelt wird, d. h. den ungefähren Standort des Benutzers,
  - Uhrzeit, Datum und Dauer der Verbindung bzw. des Verbindungsversuches.

- 1997 wurde das **Bundeskriminalamtgesetz** dahingehend geändert, daß das Bundeskriminalamt im Rahmen der Strafverfolgung zur Eigensicherung seiner Beamten Gespräche auch in Wohnungen abhören und aufzeichnen darf. Dies kann geschehen, solange sich ein Beamter in der Wohnung aufhält, aber auch „in unmittelbarem zeitlichen Zusammenhang". Außerdem können heimlich Bildaufzeichnungen hergestellt werden. Anschließend dürfen diese Aufzeichnungen zur Strafverfolgung verwendet werden.

Alles in allem wurde in den vergangenen Jahren der Leitsatz aus der Begründung zum TKG-Begleitgesetz (BT-Drucks. 13/3776), wonach **„insgesamt die lückenlose, flächendeckende und standortunabhängige Überwachung der Telekommunikation gewährleistet"** sein müsse, zielstrebig in die Tat umgesetzt.

Von dieser Flut von Abhör- und Überwachungsbefugnissen blieb als **letztes Refugium** nur die **Privatwohnung** verschont, weil das Bundesverfassungsgericht klargestellt hat, daß das Abhören von Privatwohnungen ein Eingriff in die verfassungsrechtliche Garantie der Unverletzlichkeit der Wohnung ist.

Art. 13 Grundgesetz (GG) gab dem Staat allerdings bereits in seiner bisherigen Fassung eine Eingriffsbefugnis zur Abwehr schwerer Gefahren für wichtige Rechtsgüter. Auf dieser Grundlage haben die Länder in den vergangenen Jahren in ihren **Polizeigesetzen** Abhörbefugnisse auch in Wohnungen verankert. Die Palette reicht von eng an der Verfassung orientierten Regelungen wie der schleswig-holsteinischen bis hin zu Ländern, in denen das Abhören von Wohnungen sogar zur „Vorbeugung" gegen Vergehen erlaubt wurde. 1996 entschied der Bundesgerichtshof, daß die nach den Landespolizeigesetzen zum Zwecke der Gefahrenabwehr bei Abhörmaßnahmen aus Wohnungen gewonnenen Daten auch für **Zwecke der Strafverfolgung** verwendet werden dürfen.

Diese schleichende Aushöhlung von Art. 13 GG wurde bei der Diskussion über die Einführung des **Großen Lauschangriffs** nicht etwa kritisiert, sondern umgekehrt als Argument für das Gegenteil genutzt: Man dürfe doch ohnehin nach den Landespolizeigesetzen in vielen Fällen abhören, da sei eine fehlende Abhörbefugnis für Zwecke der Strafverfolgung doch geradezu anachronistisch. Nachdem Bundestag und Bundesrat Art. 13 GG geändert haben und dadurch die Ermächtigung zum Erlaß einfachgesetzlicher Abhörbefugnisse geschaffen ist, ist keineswegs das Ende der Entwicklung erreicht. Vielmehr steht zu befürchten, daß eine neue Spirale in Gang gesetzt wurde.

Schon der erste Gesetzentwurf zur Ausführung von Art. 13 GG hält sich nicht an den Wortlaut des Grundgesetzes. Während nach der Neufassung von Art. 13 GG das Abhören von Wohnungen nur bei „**besonders schweren Straftaten**" zulässig ist, sieht das Abhörgesetz dies schon bei einfachem Bandendiebstahl vor. Obwohl das Gesetz mit der Überschrift „Organisiertes Verbrechen" operiert, enthält es in seinem Straftatenkatalog auch eine Reihe von Staatsschutzdelikten, die mit „Organisiertem Verbrechen" nichts zu tun haben. Es steht zu erwarten, daß in den kommenden Jahren der Straftatenkatalog eher erweitert als verkürzt wird. Wann immer eine Straftat in der Öffentlichkeit großes Aufsehen erregt, wird der Ruf nach der erneuten Ausweitung der Abhörmöglichkeiten ertönen. Die Forderung, daß in Privatwohnungen nicht nur Abhörmikrofone, sondern auch geheime Videokameras installiert werden dürfen, liegt bereits auf dem Tisch.

Bei der Diskussion über die Einführung des Großen Lauschangriffs spielte die Frage des Schutzes besonderer **Vertrauensverhältnisse** eine große Rolle. Zunächst ließ die Bundesregierung verlauten, das sei gar kein Problem, die besonderen Vertrauensverhältnisse seien selbstverständlich gewahrt. Wir konnten in unserer Stellungnahme aber belegen, daß nach der ständigen Rechtsprechung des Bundesgerichtshofes dem keineswegs so war. In der Folge wurden zunächst Geistliche, Abgeordnete und Strafverteidiger vom Lauschangriff ausgenommen. Im Vermittlungsausschuß ging es vornehmlich um die Erweiterung des Kreises der Berufsgruppen, die aufgrund ihres **Zeugnisverweigerungsrechts** ausgenommen werden sollten.

Bislang wurden aber zwei Dinge übersehen, die in diesem Zusammenhang berücksichtigt werden müssen: Die Zeugnisverweigerungsrechte sind nicht nur durch das Abhören von Wohnungen und Praxen gefährdet, sondern auch durch

andere **heimliche Ermittlungsmethoden**, die in den vergangenen Jahren eingeführt worden sind. So könnte beispielsweise durch einen in eine Anwaltskanzlei, Arztpraxis oder Redaktion eingeschleusten **V-Mann** das Zeugnisverweigerungsrecht der dort Tätigen umgangen werden. Es geht also um mehr als nur um die Gefährdung dieser Vertrauensverhältnisse durch den Großen Lauschangriff.

Kaum zur Sprache gekommen ist bislang, daß auch **Eheleute und** andere **Verwandte** ein **Zeugnisverweigerungsrecht** haben. Sie verfügen freilich nicht über „Berufsverbände", die öffentlichen Druck machen können. Noch 1983 hatte aber der **Bundesgerichtshof** klipp und klar festgestellt: „*Die Unterhaltung zwischen den Eheleuten ist (diesem) unantastbaren Bereich zuzurechnen. Mit der Menschenwürde läßt es sich nicht vereinbaren, wenn der Staat für sich in Anspruch nehmen könnte, die im engsten Familienbereich geführten Gespräche zu kontrollieren.*" 1996 traf der **Sächsische Staatsgerichtshof** folgende Feststellung: „*Es gibt Räume innerhalb von Wohnungen, die zu diesem absolut geschützten Bereich privater Lebensführung gehören. Es muß Räume geben, in die sich der einzelne so zurückziehen kann, daß er unangetastet von jeglicher staatlichen Einmischung seine Vorstellung von Leben nach seinem Belieben verwirklichen kann und in denen er über sein Verhalten keiner staatlichen Stelle Rechenschaft schuldet und von der Obrigkeit völlig in Ruhe gelassen werden muß. In diesem Bereich vermögen auch schwerstwiegende Interessen der Allgemeinheit oder gar einzelner einen staatlichen Eingriff nicht zu rechtfertigen.*"

Diese Aspekte wurden in der bisherigen Diskussion über den Großen Lauschangriff so gut wie gar nicht gesehen, geschweige denn wurden sie im Gesetz berücksichtigt. Es wird wohl dem Bundesverfassungsgericht vorbehalten bleiben, sie zur Geltung zu bringen. Da sie den **Schutz der Menschenwürde** betreffen, können sie auch durch ein verfassungsänderndes Gesetz mit 2/3-Mehrheit nicht entkräftet werden.

Die Diskussion um den **Großen Lauschangriff** wird also weitergehen. Sie hat bislang schon dazu geführt, daß viele Betroffene hellhörig geworden sind. Ständige Erweiterungen staatlicher Eingriffsbefugnisse zu Lasten der Privatsphäre werden künftig nicht mehr so lautlos über die Bühne gehen wie in den vergangenen Jahren. Politik und Gesellschaft werden sich mit vagen Aussagen derart, der Lauschangriff werde bestimmt „etwas bringen", auch wenn er kein „Wundermittel" sei, nicht mehr zufriedengeben. Wir brauchen endlich objektive, wissenschaftlich bewertete Zahlen über das tatsächliche Ausmaß der Bedrohung durch die Organisierte Kriminalität. Außerdem müssen wir wissen, in welchem Umfang die im Laufe der letzten Jahre kontinuierlich eingeführten neuen Eingriffsbefugnisse angewandt worden sind, wie viele Personen davon betroffen waren und welche Resultate erzielt wurden. Die Diskussion über den Großen Lauschangriff hat jedenfalls gezeigt, daß **George Orwells Vision** vom Überwachungsstaat von vielen etwas voreilig als erledigt angesehen wurde.

3. Datenschutz im Landtag

3.1 Vorschlag zur Verfassungsergänzung

Der Landtag diskutierte in einem Sonderausschuß „Verfassungsreform" eine Reihe von Vorschlägen für die Ergänzung der Landesverfassung. Wir sind der Meinung, daß eine Verfassung nicht nur bewahrenden Charakter haben darf, sondern auch die Zukunft mitgestalten muß. Deshalb haben wir die Aufnahme eines Artikels mit folgendem Wortlaut vorgeschlagen:

Artikel 9a
Teilhabe an der Informationsgesellschaft

(1) Zur Teilhabe aller an allgemein verfügbaren Informationen und an den Nutzungen der Informations- und Kommunikationstechnik fördert das Land den Erwerb der erforderlichen Kenntnisse und Fähigkeiten sowie den Aufbau einer geeigneten Infrastruktur.

(2) Informationen aus dem öffentlichen Bereich sollen allen zugänglich gemacht werden, soweit nicht schützenswerte Interessen Dritter oder das Wohl der Allgemeinheit entgegenstehen.

Wahlweise Abs. 3 oder eigener Artikel:

(3) Zur Wahrung des Rechts der Bürgerinnen und Bürger auf Schutz ihrer personenbezogenen Daten wählt der Landtag für die Dauer von sechs Jahren die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz; einmalige Wiederwahl ist zulässig. Die oder der Landesbeauftragte für den Datenschutz ist in der Ausübung des Amtes unabhängig und nur dem Gesetz unterworfen. Das nähere regelt ein Gesetz.

Absatz 1 sollte dem Ziel dienen, die Vorteile der Informationsgesellschaft nicht nur einigen wenigen, die die Informationstechnik beherrschen und über genügend Geldmittel verfügen, sich mit dieser Technik auszustatten, sondern möglichst allen zugute kommen zu lassen. Dadurch soll ein Zerfall der Gesellschaft in „information rich" und „information poor" vermieden werden.

Absatz 2 sollte das Signal zur Öffnung der Informationssammlungen der Verwaltung für alle Bürgerinnen und Bürger sein. Die skandinavischen Länder, zu denen Schleswig-Holstein eine Brückenkopffunktion einnehmen möchte, verfügen bereits über derartige Informationszugangsrechte. Soeben hat die Europäische Union in Artikel 255 des Vertrages von Amsterdam die Öffnung der Unterlagen der Kommission, des Europaparlaments und des Rates für die Bürgerinnen und Bürger der Union beschlossen. In unseren Augen ist es nur eine Frage der Zeit, bis Deutschland und die Bundesländer dem Beispiel vieler europäischer Nachbarstaaten und der USA folgen werden und allgemeine Informationszugangsrechte gewähren.

Absatz 3 sollte die Arbeit der Dienststelle des Landesbeauftragten für den Datenschutz verfassungsrechtlich absichern, so wie dies bereits in einer Reihe von Ländern geschehen ist und in Schleswig-Holstein schon bei der letzten Verfassungsreform im Jahre 1990 vorgesehen war.

Der Sonderausschuß „Verfassungsreform" hat unserem Vorschlag mehrheitlich zugestimmt und dem Plenum seine Annahme empfohlen. Dort kam leider die notwendige 2/3-Mehrheit nicht zustande.

3.2 Informations- und Kommunikationsnetz im Landtag

Auf Initiative der Landtagsverwaltung ist Ende 1997 eine Arbeitsgruppe gebildet worden, in der Mitarbeiter der IT-Leitstelle des Landtages und Spezialisten unseres Technikreferates die Sicherheitsfragen bei der Einführung eines Informations- und Kommunikationsnetzes im Landtag durchleuchten. Aus unserer Sicht hat diese Beratungsmaßnahme eine **Pilotfunktion** im Hinblick auf den Aspekt der mehrseitigen Datensicherheit. In kaum einem anderen öffentlichen Bereich muß ein IT-System eine so große Anzahl **unterschiedlicher Sicherheitsinteressen** berücksichtigen. Neben den typischen Verwaltungsaufgaben (z. B. Haushaltsplanung, Haushaltsvollzug) sollen nach unserer Kenntnis auch so „brisante" Komplexe wie z. B. Personaldatenverwaltung der Mitarbeiter, Abwicklung der finanziellen Ansprüche der Abgeordneten, externe und interne IT-Kommunikation der Fraktionen, Anschluß an das CAMPUS-Netz und dessen Services, Verbindung mit dem Internet über das Schleswig-Holstein-Netz der Datenzentrale, Abschottung von Teilnetzen und Datenbeständen der verschiedenen Benutzerkreise abgedeckt werden.

Wir werden zunächst eine umfassende Bestandsaufnahme aller bisher realisierten hard- und softwaretechnischen Komponenten vornehmen und die derzeitigen und künftigen Anforderungen der Nutzer der Systeme ermitteln. Hieraus wird dann ein Sicherheitskonzept abzuleiten sein, das allen Beteiligten aufzeigt, welche Dienstleistungen die Informationstechnik im Landtag unter welchen Rahmenbedingungen erbringen kann und wie die Sicherheitsanforderungen der Beteiligten erfüllt werden können. Wir werden unser besonderes Augenmerk darauf richten, daß die Ergebnisse aufbereitet werden und für die einzelnen Abgeordneten und die Fraktionen als Entscheidungshilfe dienen können.

4. Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Modellprojekt Bürgerbüro

Auch in Bürgerbüros muß der Datenschutz beachtet werden. Die Gemeinde Altenholz versucht dies in einem Modellprojekt zu verwirklichen. Wir begleiten das Vorhaben beratend.

„Wer Bürgerbüros einrichten möchte, muß sicherstellen, daß dabei nicht der Datenschutzservice verschlechtert wird." So schlossen unsere Ausführungen zum **Bürgerbüro** im letzten Tätigkeitsbericht (19. TB, Tz. 4.1.4). Wir hatten damals mit einigen Gemeinden Gespräche geführt und waren auf Probleme bei der Zweckbindung personenbezogener Daten gestoßen, auf Fragen der Abschottung unterschiedlicher kommunaler Aufgabenbereiche voneinander und auf Risiken, die bei der „offenen" Beratung im Bürgerbüro auftreten.

Inzwischen sind wir von der Gemeinde Altenholz gebeten worden, sie bei der Organisation ihres Bürgerbüros zu beraten und die eingeleiteten Maßnahmen unter datenschutzrechtlichen Gesichtspunkten kritisch zu betrachten. Dabei ging es insbesondere um folgende Fragen:

- Welche Aufgaben werden im Bürgerbüro erfüllt? Besteht die Gefahr unzulässiger Verwendung von Daten, die zu unterschiedlichen Zwecken erhoben wurden?
- Werden die Besucher des Bürgerbüros über dessen Arbeitsweise ausreichend aufgeklärt und darüber unterrichtet, daß und wann die mehrfache Nutzung ihrer Angaben für unterschiedliche Zwecke von ihrer Einwilligung abhängt?
- Ist die räumliche Ausstattung des Bürgerbüros so, daß die Kenntnisnahme von personenbezogenen Daten durch Dritte ausgeschlossen ist bzw. werden kann?

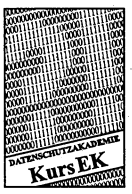
Es zeigte sich, daß eine **abschließende Bearbeitung** durch das Bürgerbüro nur bei Meldeangelegenheiten erfolgt. In allen anderen Fällen werden Anträge entgegengenommen und die Bürger beraten. Die abschließende Bearbeitung und Entscheidung der Vorgänge erfolgt dann in den jeweiligen Fachämtern. Für die Bereiche Bauamt und Sozialhilfe sind nach wie vor ausschließlich die Fachämter zuständig. Ihre Aufgaben sind zu komplex und zu schwierig, um sie mit der vorhandenen Personalkapazität im Bürgerbüro erledigen zu können.

Besucher des Bürgerbüros werden darüber aufgeklärt, daß eine Weiterverarbeitung ihrer Daten durch die Gemeinde nur soweit erfolgt, wie sie es wünschen. Allerdings werden sie auch auf eventuell bestehende Meldepflichten gegenüber der Verwaltung hingewiesen. Zu Problemen mit den Zweckbindungsvorschriften des Datenschutzes ist es nach Angaben der Gemeinde bisher noch nicht gekommen.

Wir haben empfohlen, die **Einwilligung** der Bürger zur Weiterverarbeitung ihrer Daten nicht nur mündlich einzuholen, sondern sie auch zu dokumentieren. Es ist nämlich leicht möglich, dem Bürger an Ort und Stelle schriftlich zu bescheinigen, welche Anträge rechtswirksam gestellt wurden (Antrag auf Zuteilung einer Mülltonne, Anmeldung eines Hundes, Mitteilung einer Bankverbindung u. ä.) bzw. welche Maßnahmen aufgrund seines Besuches veranlaßt wurden. Ein Exemplar dieses Nachweises könnte von ihm unterschrieben und im Bürgerbüro abgelegt werden. So wäre auch die Herkunft der Daten nachzuweisen, gleichzeitig könnte über Art und Zweck der Datenerhebung aufgeklärt werden.

Die Gemeinde will diese Anregungen aufgreifen. Darüber hinaus ist neben der mündlichen **Aufklärung** der Betroffenen zusätzlich ein Merkblatt über die Bedeutung des Zweckbindungsgrundsatzes erstellt worden, das die Bürger über die Grenzen einer zulässigen Datenverarbeitung durch die Verwaltung aufklärt. Es wird im Bürgerbüro ausgelegt. Die Besucher können so bei entsprechendem Interesse in Ruhe nachlesen, in welchem Umfang sie mit einer Verarbeitung ihrer Daten durch die Gemeinde rechnen müssen.

Bei unserem Besuch konnten wir schließlich feststellen, daß in dem Großraumbüro mit drei Arbeits- und Besprechungsplätzen auf den Tischen ein deutlicher Hinweis angebracht war, daß für eine vertrauliche Beratung der jeweiligen Angelegenheit auch ein **gesondertes Besprechungszimmer** zur Verfügung stehe.



Nach diesem überwiegend positiven Eindruck vom Vorgehen der Gemeinde haben wir verabredet, uns mit datenschutzrechtlicher Beratung auch an dem **Fortgang des Projektes** zu beteiligen. Als weitere Entwicklung ist u. a. ein Zugriff der Bürger zu Informationsangeboten der Gemeinde in automatisierten Systemen beabsichtigt.

Was ist zu tun?
Kommunen, die den Bürgern mit mehr Service entgegenkommen wollen, müssen auch die datenschutzrechtlichen Anforderungen beachten. Sie können sich dabei gerne von uns beraten lassen.

4.1.2 Bauleitplanung und Öffentlichkeit von Einwendungen

Bebauungspläne werden als Satzungen in einem öffentlichen Verfahren aufgestellt. Personenbezogene Informationen der Beteiligten können aber ausnahmsweise durch Ausschluß der Öffentlichkeit bei den Beratungen vertraulich behandelt werden.

Flächenbezogene Planungen der Kommune berühren fast immer eine Mehrzahl von Bürgern. Das gilt, wenn jemand sein Wohnhaus baut und der Nachbar voller Interesse beobachtet, „was da auf ihn zukommt", wenn eine Straße projektiert wird und im Planfeststellungsverfahren die Beteiligten Gelegenheit haben, Einwendungen gegen das konkrete Bauvorhaben zu erheben und wenn Bauleit-

pläne entwickelt und in Beratungen Anregungen und Bedenken der Bürger abgewogen werden. Stets erhebt sich dabei die Frage, welche **Daten der Beteiligten** anderen bekannt werden dürfen oder gar veröffentlicht werden müssen und wieweit ein Anspruch auf die diskrete Behandlung persönlicher Betroffenheit besteht.

So fragte eine Stadt bei uns an, ob die Anregungen und Bedenken zu dem Entwurf eines Bebauungsplanes den Mitgliedern der **Stadtvertretung** und der **Ausschüsse** für ihre Beratungen nur in anonymisierter Form zugeleitet werden dürften oder ob im Hinblick auf die Verschwiegenheitspflicht der Stadtvertreter eine Namensnennung unschädlich sei, wenn für die Beratungen die Öffentlichkeit ausgeschlossen werde. Die Stadt wies zugleich darauf hin, daß eine wirkliche Anonymisierung der Anregungen schwierig sein könne, wenn diese die Art der Betroffenheit deutlich machten und schon dadurch die Identität des Einwenders erkennbar würde. Darüber hinaus schreibe ein Erlaß des Innenministeriums über das Verfahren bei der Aufstellung von Bauleitplänen die öffentliche Beratung der Einwendungen ausdrücklich vor.

Die Bauleitplanung der Gemeinden ist eine „Normsetzung", die aufgrund des Kommunalverfassungsrechts vom **Grundsatz der Publizität** beherrscht wird. Über Anregungen zu und Einwendungen gegen Bebauungspläne wird nach dem Baugesetzbuch in den kommunalen Entscheidungsgremien beschlossen und zwar grundsätzlich in öffentlicher Sitzung. Die Öffentlichkeit der Sitzungen kann nur unter den Voraussetzungen, die die Gemeindeordnung dafür festlegt, ausgeschlossen werden. Die Öffentlichkeit ist demnach im konkreten Einzelfall dann auszuschließen, „wenn ... berechtigte Interessen einzelner es erfordern". Dies ist der Fall, wenn aus der Diskussion über Einwendungen persönliche Verhältnisse in einem besonderen Maße offenbart würden.

Auch Unterlagen, die den Gemeindevertretern für die Beratungen zur Verfügung gestellt werden, dürfen einen Personenbezug nur enthalten, soweit dies notwendig ist. In der Regel wird sich aber nicht immer vermeiden lassen, daß Einwendungen den Mitgliedern der Gremien **personenbezogen** vorzulegen sind, weil anders die Bedenken und die Betroffenheit der einzelnen Bürger nicht beurteilt werden können. Das informationelle Selbstbestimmungsrecht des Einwenders ist durch die Pflicht der Gemeindevertreter geschützt, „über die ihnen bei dieser Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren".

Was ist zu tun?
Für die Erörterung von Bauleitplänen sind den kommunalen Gremien soweit erforderlich die Anregungen Betroffener in personenbezogener Form zugänglich zu machen. Die Beratungen sind grundsätzlich öffentlich. Sie sind allerdings so zu führen, daß die Offenbarung personenbezogener Daten soweit möglich vermieden wird. Die Öffentlichkeit ist auszuschließen, soweit berechtigte Interessen der Einwender es erfordern.

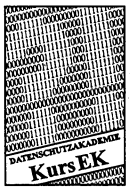
4.1.3 Der Umgang der Mandatsträger mit Sitzungsunterlagen

Sitzungsunterlagen für kommunale Mandatsträger sind Unterlagen der Kommunen und unterliegen den Löschungsvorschriften des Datenschutzrechts.

Ein Disziplinarverfahren gegen den Mitarbeiter einer Kommune endete, ohne daß eine Disziplinarmaßnahme ausgesprochen wurde. Nach dem Personalaktenrecht mußten folglich die entstandenen Vorgänge aus der **Personalakte** entfernt und vernichtet werden, da sich die erhobenen Vorwürfe als unbegründet herausgestellt hatten. Allerdings waren eine Reihe von Unterlagen auch Mandatsträgern im Rahmen der Beratung des Falles in den gemeindlichen Gremien zur Verfügung gestellt worden.

Entgegen der weitverbreiteten Auffassung von Mandatsträgern gehören Sitzungsvorlagen nicht zu ihren privaten Unterlagen. Es handelt sich vielmehr um Daten, die sie ausschließlich in ihrer Eigenschaft als **Funktionsträger** erhalten. Als Mitglied in einem politischen Entscheidungsgremium tragen sie zur Aufgabenerfüllung der Kommune bei. Die Vertretungskörperschaft ist als datenverarbeitende Stelle im datenschutzrechtlichen Sinne anzusehen.

Auch für sie gelten die **datenschutzrechtlichen Löschungsregelungen**. Deshalb sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange der oder des Betroffenen beeinträchtigt werden.



Im konkreten Fall war die Löschung zur Wahrung schutzwürdiger Belange des Betroffenen geboten. Die Mandatsträger mußten die Sitzungsvorlagen über das Disziplinarverfahren vernichten.

Was ist zu tun?
Die Kommunen haben dafür Sorge zu tragen – im Rahmen einer Satzung –, daß ihre Mandatsträger personenbezogene Daten nur solange aufbewahren, wie es für ihre rechtmäßige Aufgabenerfüllung erforderlich ist. Die Einzelheiten könnten geschäftsordnungsmäßig in einer „Datenschutzdienstanweisung für Mandatsträger" festgelegt werden.

4.1.4 Wenn Detektive Ordnungswidrigkeiten ermitteln

Privatdetektive dürfen nicht zielgerichtet Tatsachenermittlung für Ordnungswidrigkeitenverfahren – z. B. im Zusammenhang mit der Kurtaxe – betreiben.

Eine Fremdenverkehrsgemeinde in Schleswig-Holstein hatte eine Detektei beauftragt, Ermittlungen und Kontrollen zu Verstößen gegen die Kurabgabesatzung durchzuführen. Mitarbeiter der **Detektei** befragten auf der Straße Passanten u. a., ob sie Kurgäste seien, eine Kurkarte besäßen und wer ihr Vermieter sei. Auf der Grundlage dieser Ermittlungen sollten Ordnungswidrigkeiten der Vermieter festgestellt und geahndet werden. Der örtliche Bürger- und Vermieterverein bat uns, die Zulässigkeit einer solchen „Privatisierung" zu prüfen.

Wir hatten gravierende Bedenken gegen diese Form der Datenerhebung. Die gezielte **Tatsachenermittlung** zum Nachweis von **Ordnungswidrigkeiten** ist mit der Durchführung von Bußgeldverfahren so eng verbunden, daß sie mit dieser untrennbar zum Gesamtkomplex der **hoheitlichen Aufgaben** gehört. Zwar ist eine Übertragung hoheitlicher Aufgaben unter bestimmten Voraussetzungen möglich. Sie setzt jedoch eine ausdrückliche Beleihung auf gesetzlicher Grundlage voraus. Eine Grundlage fehlt im vorliegenden Fall. Bloße Verwaltungshilfe scheidet ebenfalls aus. Denn die planmäßige Ermittlung und Dokumentation von Verstößen gegen die Satzung steht in einem unmittelbaren Zusammenhang mit der originären Aufgabe der Verfolgung und Ahndung von Ordnungswidrigkeiten. Sie kann nach der Rechtsprechung deshalb auch dann nicht auf private Auftragnehmer übertragen werden, wenn die zuständige Behörde Ort, Zeit und Umfang der Kontrollen bestimmt und der einzelne Mitarbeiter direkt den Weisungen des Auftraggebers unterworfen ist. Wir haben die gewählte Form der Datenerhebung nach alledem beanstandet.

Was ist zu tun?
Dient eine Datenerhebung durch Private unmittelbar der Verfolgung von Ordnungswidrigkeiten, so ist sie untrennbarer Bestandteil hoheitlicher Tätigkeit und darf nur nach ausdrücklicher Beleihung erfolgen.

4.1.5 Grenzen für den Vollstreckungsbeamten

Ein Vollstreckungsbeamter darf den Vermieter des Schuldners nicht über Einzelheiten der Zwangsvollstreckung unterrichten.

Der Zweck heiligt nicht immer die Mittel; dies mußte schließlich auch ein kommunaler Vollstreckungsbeamter einsehen. Nachdem die Mahnung wegen einer Forderung über 100 DM beim Betroffenen keinen Erfolg gezeigt hatte, wandte er sich kurzerhand an den Vermieter des Zahlungspflichtigen und stellte eine richterliche Durchsuchung der Wohnung in Aussicht, die gegebenenfalls auch mit einer zwangsweisen Öffnung der Tür verbunden gewesen wäre. In

diesem Zusammenhang offenbarte er gegenüber dem Vermieter **Details** aus dem **Vollstreckungsverfahren**. Durch diese Unterrichtung des Vermieters sollte wohl auch erreicht werden, daß dieser den Zahlungspflichtigen drängen sollte, seine Schuld zu begleichen.

Zwar dürfen Vollstreckungsbeamte im Rahmen ihrer Ermittlungstätigkeit Daten bei Dritten erheben. Dies darf jedoch nicht dazu führen, daß Daten aus dem Zwangsvollstreckungsverfahren den Dritten gegenüber offenbart werden. Geschieht dies dennoch, liegt möglicherweise ein strafrelevanter Sachverhalt, zumindest ein Verstoß gegen das Datengeheimnis (§ 6 LDSG) vor. In dem geprüften Fall war die unbefugte Offenbarung personenbezogener Daten gegenüber dem Vermieter zu beanstanden.

Was ist zu tun?
Vollstreckungsbeamte brauchen Durchsetzungsvermögen, aber auch ein Gespür für die Sensibilität des Vorgangs für den Schuldner.

4.2 Polizei

4.2.1 Staatsschutz macht „klar Schiff"

Nach einer Prüfung im Staatsschutzdezernat des Landeskriminalamtes wurden umfangreiche Bereinigungen des Datenbestandes in Angriff genommen. Von ursprünglich 6 000 Personenakten sind noch 1 362 übriggeblieben. Fast alle strittigen Fragen wurden inzwischen datenschutzgerecht gelöst. In einigen Punkten besteht aber noch Streit.

Die Aufarbeitung der Querschnittsprüfung, über die wir im 19. Tätigkeitsbericht (Tz. 4.2.1) ausführlich berichteten, gemeinsam mit dem Innenminister und dem Landeskriminalamt verlief insgesamt kooperativ und zügig. Der dabei in Gang gesetzte Klärungsprozeß hat nicht nur zu **gravierenden Verbesserungen** bei der Umsetzung der Datenverarbeitungsbestimmungen des Landesverwaltungsgesetzes (LVwG), sondern aufgrund einer zielgerichteten Datenreduzierung zu einem aufgabengerechten nutzbaren Bestand an Informationen beim Staatsschutz geführt. Die Zahl der Personenakten wurde von ca. 6 000 auf 1 362 reduziert.

- Als Ergebnis der Prüfung wird die Struktur der Personenakten im Staatsschutzdezernat derjenigen der herkömmlichen Kriminalakten angeglichen.
- Zukünftig werden die Informationen in Form von Merkblättern gespeichert, die nur die zur Prävention erforderlichen Angaben enthalten.
- Die Fristenprüfung bei den Personenakten wird automatisiert überwacht.
- Die Einhaltung der Vorgaben über die Datenspeicherung zur Vorbeugung wird künftig gewährleistet: Insbesondere dürfen Daten zur vorbeugenden Bekämpfung von Straftaten nur bei Vorliegen entsprechender Tatsachen gespeichert werden und nicht wie bisher bei Vermutungen.

- Sogenannte Gruppendelikte, deren Zuordnung zu einem bestimmten Täter innerhalb der Gruppe nicht möglich war, dürfen nur zu den Personen gespeichert werden, die mindestens einer Teilnahme an der Tat verdächtigt sind.
- Neue Maßstäbe gelten für die Speicherung von „ergänzenden Erkenntnissen", die regelmäßig in der Akte zu begründen ist, etwa wenn sie ausnahmsweise dritte Personen oder legale Grundrechtsausübungen betrifft.
- Der Verbleib von Lichtbildern wird in einem neuen Verfahren lückenlos dokumentiert.
- Die Akten über gefährdete Personen werden bereinigt und künftig jährlich überprüft.
- Der Altbestand an sogenannten Institutionenakten wird insgesamt vernichtet, und es wird eine neue Institutionenkartei aufgebaut, die präzise nach Sachverhalten der Gefährdungsanalyse und der kriminalpolizeilichen Sammlungen aufgeteilt ist.
- Innen- und Justizministerium werden das Verfahren der Häftlingsüberwachung neu regeln; die Unterlagen aus abgeschlossenen Häftlingsüberwachungen – insbesondere Kopien der teilweise äußerst sensiblen Briefe an über wachte Gefangene – werden vernichtet.

Offen ist zum einen nach wie vor das Problem, inwieweit **Durchschriften** aus nicht vom Staatsschutzdezernat des LKA selbst bearbeiteten staatsschutzrelevanten Vorgängen dort aufbewahrt werden dürfen. Hierzu wird eine gemeinsame Lösung im Rahmen der anstehenden Novellierung der Strafprozeßordnung (StPO) durch das Strafverfahrensänderungsgesetz (StVÄG) erarbeitet werden müssen.

Strittig ist außerdem die Frage der dauerhaften Speicherung und Nutzung von **Lichtbildern**, die der Staatsschutz dem Personalausweis- oder Paßregister entnommen hat: Es ist dort gängige Praxis, sich zur Vorbereitung einer Observation, bei einer sich konkretisierenden Gefahr oder zur Durchführung eines Strafverfahrens ein Lichtbild aus dem **Paß- bzw. Personalausweisregister** zu besorgen, welches nach Abschluß des Vorganges in die allgemeine Lichtbildkartei des Staatsschutzdezernates aufgenommen wird, sofern zur betroffenen Person auch eine Personenakte geführt wird. Nach unserer Auffassung hat dies die Qualität einer **erkennungsdienstlichen Maßnahme.** Wir fordern deshalb, daß die für die Verarbeitung von Lichtbildern geltenden besonderen Voraussetzungen der Strafprozeßordnung und des Landesverwaltungsgesetzes nicht umgangen werden dürfen. Gegenüber der ed-Behandlung hat das beschriebene Verfahren für den Betroffenen den zusätzlichen Nachteil, daß er von der Verarbeitung seines Lichtbildes, das er für ein völlig anderes Verwaltungsverfahren hergegeben hat, durch die Polizei nichts weiß. Nach unserer Auffassung müssen die Betroffenen deshalb, wie stets bei einer verdeckten Anfertigung von Bildaufnahmen, grundsätzlich nach Abschluß der Maßnahme hiervon unterrichtet werden.

Der Innenminister hingegen will die Verarbeitung der Paß- bzw. Personalausweisbilder auf die allgemeinen, für alle Arten von Daten geltenden Generalklauseln der StPO bzw. des LVwG stützen. Dies wird nach unserer Auffassung dem schweren Informationseingriff, der in einer Verarbeitung eines Lichtbildes liegt, nicht gerecht.

Was ist zu tun?
Zur Häftlingsüberwachung muß eine neue Verfahrensweise zwischen Justiz- und Innenminister unter unserer Beteiligung abgestimmt werden. Auch die Aufbewahrung von Vorgangsdurchschriften im Staatsschutzdezernat ist neu zu regeln. Bei der Verarbeitung von Lichtbildern aus Paß- und Personalausweisregistern müssen die polizeirechtlichen Anforderungen an ed-Maßnahmen eingehalten werden.

4.2.2 Ein Bürger, das Bundeskriminalamt, INTERPOL und die kanadische Polizei

Als er einen Einwanderungsantrag stellte, verfing sich ein Bürger im Informationsgeflecht zwischen Landespolizei, Bundeskriminalamt, INTERPOL und kanadischen Polizeibehörden. Dabei zeigte sich, daß die Informationswege effektiv genug waren, um seine Einbürgerung zu verhindern, jedoch versagten, als es um die Korrektur der Datenbestände ging.

Ein aus Schleswig-Holstein stammender Petent hatte in Kanada einen Einwanderungsantrag gestellt. Kurz darauf wurde ihm mitgeteilt, daß die Einwanderungsbehörde über eine **INTERPOL-Anfrage** polizeiliche Datenspeicherungen in Deutschland über ihn festgestellt habe, die einer Einbürgerung im Wege stünden. Welcher Art diese Eintragungen waren und woher sie rührten, sollte nun vom Petenten selbst geklärt werden. Er begab sich zurück nach Deutschland und wandte sich mit der dringenden Bitte an uns, ihm – der nicht vorbestraft war – bei der Suche nach polizeilichen Datenbeständen zu helfen. Bald schon war geklärt, daß es solche Bestände bei der schleswig-holsteinischen Landespolizei nicht (mehr) gab, daß jedoch das Bundeskriminalamt noch Speicherungen betreffend dreier Ermittlungsverfahren gegen den Petenten aus den Jahren 1982 bis 1989 vorhielt, ohne daß dort eine strafrechtliche Verurteilung bekannt war. Das Aussonderungsprüfdatum, an dem entschieden werden sollte, ob eine weitere Speicherung noch erforderlich oder die Aufzeichnungen zu löschen waren, ist vom Bundeskriminalamt zunächst auf den 30.04.1994 festgesetzt worden. Wenige Tage später ging die Information von INTERPOL-Kanada ein, daß dort ein Verfahren wegen eines Rauschgiftvergehens gegen den Petenten anhängig sei. Diesen Vorgang nahm das Bundeskriminalamt zum Anlaß, die Aussonderungsprüffrist um 10 Jahre in das Jahr 2004 hinein zu verlängern.

Wir baten das Bundeskriminalamt, sich umgehend mit **INTERPOL-Kanada** in Verbindung zu setzen, um den Ausgang des von dort mitgeteilten kanadischen Verfahrens zu klären, denn hiervon war die für das Einwanderungsverfahren bedeutsame Frage abhängig, ob die beim Bundeskriminalamt gespeicherten Daten

über den Petenten noch vorgehalten werden durften. Das Bundeskriminalamt versuchte nun nach eigenen Angaben seit Mitte September 1996 eine Antwort von INTERPOL-Kanada zu erhalten – jedoch ohne Erfolg. Obwohl der Bundesbeauftragte für den Datenschutz und wir beim Bundeskriminalamt ständig nachhakten, dauerte es ein ganzes Jahr bis zur Auskunft, daß das Ermittlungsverfahren in Kanada zwischenzeitlich ausgesetzt wurde. Die weitere Anfrage des Bundeskriminalamtes nach näheren Tatumständen bzw. einem zwischenzeitlichen Ausgang des Verfahrens blieb bislang unbeantwortet.

Aufgrund der nicht nachvollziehbaren Verzögerungen auf dem INTERPOL-Kommunikationsweg konnte dem Petenten also noch nicht geholfen werden. Der polizeiliche Informationsaustausch zwischen Landespolizei, Bundeskriminalamt und kanadischen Polizeibehörden hatte gut genug funktioniert, um den Petenten belastende verdachtsbezogene Daten auszutauschen und zu speichern; bei der – wie sich im Einwanderungsverfahren zeigte – im Interesse des Betroffenen dringend erforderlichen Abklärung dieser „weichen" Daten jedoch erwies sich INTERPOL bislang als **träge und bürokratisch**. Seit über drei Jahren ist man nicht in der Lage zu klären, was an den alten Verdachtsmomenten gegen den Petenten wirklich dran ist. Der wartet seitdem vergeblich auf seine Einbürgerung. Kein gutes Omen für andere Bereiche der internationalen polizeilichen Zusammenarbeit wie etwa EUROPOL!

Was ist zu tun?
Die internationalen Informationsverbindungen der Polizei müssen so gestaltet werden, daß nicht nur Verdachtsgründe blitzschnell mitgeteilt, sondern auch entlastende Informationen zügig übermittelt werden.

4.2.3 Immunität für EUROPOL-Mitarbeiter?

Die Europäische Polizeibehörde EUROPOL soll Vorrechte und ihre Mitarbeiter Immunitäten erhalten. Damit wird der Bürger gegenüber den ohnehin schon weitreichenden Befugnissen dieser Stelle noch mehr benachteiligt.

Im 18. Tätigkeitsbericht (Tz. 4.2.9) haben wir uns kritisch mit den Befugnissen von EUROPOL auseinandergesetzt. Die Bundesregierung hat nunmehr einen Gesetzentwurf über die Vorrechte und Immunitäten für EUROPOL vorgelegt. Danach würden EUROPOL-Mitarbeiter hinsichtlich unzulässiger oder unrichtiger Datenverarbeitung sowie der von ihnen in Ausübung ihres Amtes vorgenommenen mündlichen und schriftlichen Äußerungen sowie Handlungen eine weitgehende **Immunität** erhalten. Hierdurch soll die Unabhängigkeit und Funktionsfähigkeit von EUROPOL gewährleistet werden. Als Begründung wird außerdem angegeben, daß sich die Behörde gegenwärtig im wesentlichen auf die Informationsverarbeitung beschränke und keine exekutiven Funktionen erfülle, so daß die Aufgaben nicht mit denen der Polizei des Bundes und der Länder, die derartige Vorrechte und Immunitäten nicht besitzen, identisch seien.

Diese Argumentation vermag jedoch nicht zu überzeugen. Auch wenn EUROPOL noch nicht im Besitz der ansonsten für die Polizei üblichen Zwangsbefugnisse ist, bleibt festzustellen, daß gerade im Rahmen der Verarbeitung personenbezogener Angaben erhebliche Schäden verursacht werden können – etwa wenn polizeiliche Erkenntnisse unzulässigerweise an Dritte weitergegeben werden und der Betroffene dadurch z. B. wirtschaftliche Einbußen erleidet. Von daher ist es **nicht nachvollziehbar**, daß EUROPOL besser gestellt werden soll als einzelstaatliche Institutionen. Denn bei diesen kommt auch niemand auf die Idee, daß ihre Funktionsfähigkeit durch das allgemein geltende Haftungsrecht eingeschränkt sein könnte. Die Bestimmungen haben außerdem den Nachteil, daß die Tätigkeit der Kontrolleure von EUROPOL, die wiederum von der Immunität ausgenommen sind, erheblich beeinträchtigt werden könnte. Denn angesicht der weitgehenden Immunitäten und Vorrechte der EUROPOL-Mitarbeiter ist eine effektive Kontrolle vom Goodwill der jeweiligen Einheit, die überprüft werden soll, abhängig.

Was ist zu tun?
Die Landesregierung sollte das Immunitäten-Protokollgesetz in der gegenwärtigen Form im Bundesrat ablehnen.

4.2.4 Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS

Für die vom Bundeskriminalamt geführte automatisierte Fingerabdruck-Datei wurde der Entwurf einer Errichtungsanordnung vorgelegt, die jedoch in vielen Punkten überarbeitungsbedürftig ist.

Das AFIS wird beim Bundeskriminalamt und den Länderpolizeien eingesetzt, um eine Identifizierung unbekannter Personen zu ermöglichen. In der Datei werden Fingerabdrücke von mutmaßlichen Straftätern, aber auch von Asylbewerbern und von sonstigen Personen, die nach dem Ausländergesetz erkennungsdienstlich behandelt worden sind, automatisiert gespeichert. Obwohl das Verfahren bereits seit 1992 angewendet wird, gibt es hierfür bislang keine **Errichtungsanordnung**, in der festgelegt ist, welche Daten im einzelnen eingegeben werden dürfen, wer zugriffsberechtigt ist und wann die Daten wieder zu löschen sind.

? ***AFIS***

AFIS ist eine Zentraldatei, die beim Bundeskriminalamt geführt wird. Zugriffsberechtigt sind aber auch die Landeskriminalämter. Die Datei dient dazu, durch einen automatisierten Vergleich von Fingerabdruckdaten, die z. B. an einem Tatort aufgefunden werden, den Spurenverursacher zu identifizieren. Außerdem kommt das System bei der Überprüfung von Asylbewerbern und Ausländern zum Einsatz.

Auf Drängen der Datenschutzbeauftragten von Bund und Ländern hat das Bundeskriminalamt im Sommer dieses Jahres endlich den Entwurf einer solchen Errichtungsanordnung vorgestellt. Dieser gab insbesondere in folgenden Punkten Anlaß zu Kritik:

- Der **Personenkreis**, über den Daten gespeichert werden, ist nicht, wie es gesetzlich erforderlich ist, konkretisiert.
- Es ist nicht sichergestellt, daß Fingerabdrücke, die nach dem Ausländergesetz und dem Asylverfahrensgesetz erhoben worden sind, von den erkennungsdienstlichen Unterlagen mutmaßlicher Straftäter **getrennt aufbewahrt** werden, wie es das Asylverfahrengesetz und das Ausländergesetz ausdrücklich verlangen.
- Die **Protokollierung** der Abrufe läßt nicht erkennen, nach welcher Rechtsgrundlage sich die Recherchen gerichtet haben; dadurch kann eine nachträgliche Rechtmäßigkeitskontrolle nicht sinnvoll durchgeführt werden.
- Die Regelungen waren noch nicht an die seit dem 01.08.1997 geänderten Bestimmungen des **Bundeskriminalamtgesetzes** angepaßt.

Nachdem eine Reihe von Ländern, dem Entwurf die erforderliche Zustimmung verweigerten, hat der Bundesinnenminister das Bundeskriminalamt mit der Ausarbeitung neuer Errichtungsanordnungen, getrennt für die Strafermittlungs- und Asylbereiche von AFIS, beauftragt.

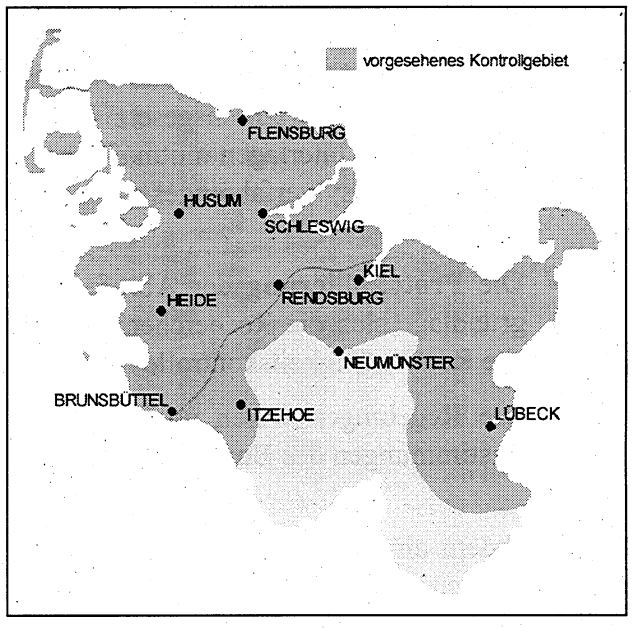
Was ist zu tun?
Die AFIS-Errichtungsanordnung sollte unter Berücksichtigung der o. g. Aspekte schleunigst überarbeitet werden.

4.2.5 Schleierfahndung

Mit dem Schengener Abkommen verpflichten sich die Unterzeichnerstaaten, die Grenzkontrollen untereinander abzubauen, dafür an den Außengrenzen verstärkt zu kontrollieren und illegale Einwanderung und Grenzübertritte zu verhindern. Gleichwohl befürchtete Sicherheitseinbußen sollen in Schleswig-Holstein durch „Schleierfahndungen" ausgeglichen werden. Hiergegen bestehen allerdings datenschutzrechtliche Einwände.

Anlaß für die Beschäftigung mit dieser Problematik war ein Gesetzentwurf der Landtagsfraktion der CDU aus dem Januar 1997. Um die Sicherheitsdefizite, die durch den absehbaren Wegfall der Kontrollen an der Grenze zu Dänemark im Land Schleswig-Holstein befürchtet wurden, auszugleichen, sah der Gesetzentwurf vor, in das Landesverwaltungsgesetz eine neue Befugnis zur **anlaßfreien Personenkontrolle** aufzunehmen.

Nach der geltenden Rechtslage bedarf die Polizei konkreter Anhaltspunkte, um eine Identitätsfeststellung vornehmen zu können. Dabei reicht es aus, daß im Einzelfall eine Gefahr vorliegt oder eine Person sich an gefährlichen oder gefährdeten Orten, die im Gesetz näher bezeichnet sind, aufhält oder Tatsachen für die Begehung bestimmter Straftaten sprechen.



Nach dem Gesetzentwurf sollten darüber hinaus die Identitätskontrollen ohne weitere Begründung in einem Gebiet vorgenommen werden dürfen, das sich von der Grenze zu Dänemark und den Küsten aus jeweils 30 km landeinwärts erstreckt, sowie in den Gegenden 10 km landeinwärts von den Ufern des Nord-Ostsee-Kanals und auf Durchgangsstraßen und in öffentlichen Einrichtungen des internationalen Verkehrs. Diese Befugnisse, die bereits in ähnlicher Form in Baden-Württemberg und Bayern in das Polizeirecht aufgenommen wurden, sollen einen „Sicherheitsschleier" über die erfaßten Gebiete werfen. Deswegen wird sie im allgemeinen als „**Schleierfahndung**" bezeichnet.

Auf Ersuchen des Innen- und Rechtsausschusses haben wir in einer Stellungnahme die folgenden rechtsstaatlichen Bedenken geltend gemacht:

- Begründet wird die Schleierfahndung mit dem Wegfall der Personenkontrollen an den Landesgrenzen. Tatsächlich führt aber die Befugnis, in einem tief ins Landesinnere hineinreichenden Gebiet kontrollieren zu dürfen, zu einem **grundsätzlich anderen Instrument**, als es die Kontrolle beim Grenzübertritt darstellt. Dies zeigt sich insbesondere, wenn auf der Karte des Landes Schleswig-Holstein das Gebiet abgesteckt werden soll, das von der Schleierfahndung erfaßt werden würde. Jedenfalls im Landesteil nördlich des Nord-Ostsee-Kanals wäre mit Ausnahme eines kleinen Innenbereichs nahezu das gesamte Landesgebiet betroffen.
- Das Instrument der Schleierfahndung ist konzipiert als Kompensation für den Wegfall der Grenzkontrollen im Zusammenhang mit dem Schengener Abkommen. Eine **Kompensation** ist jedoch bereits im Schengener Durchführungsübereinkommen selbst vorgenommen worden. Neben den verstärkten Kontrollen an den Außengrenzen sind im sogenannten „Schengenraum" grenzüberschreitende Observationen und vor allem die Nacheile, d. h., das Recht der Polizeibeamten des einen Landes, flüchtige Täter über die Grenzen hinweg verfolgen zu dürfen, vorgesehen. Neu eingerichtet wurde das **Schengener**

Informationssystem, das Fahndungsdaten in erheblichem Umfang im gesamten Schengengebiet für alle beteiligten Polizeien zum Abruf bereithält. Eine weitere Maßnahme im Hinblick auf Schengen würde unseres Erachtens zu einer Überkompensation führen.

- Dürfen Personenkontrollen **anlaßfrei**, d. h. ohne gesetzlich genannte Voraussetzungen durchgeführt werden, so tritt an die Stelle genau definierter Tatbestände der „polizeiliche Instinkt" des einzelnen Beamten vor Ort. An die Stelle bestimmter Eingriffstatbestände würde Ermessen treten, das kaum noch gerichtlich überprüft werden könnte. Das Verhältnis der Bürger zur Polizei würde sich verändern, wenn diese damit rechnen müßten, jederzeit zum Objekt polizeilichen Handelns gemacht werden zu können, ohne eine Veranlassung dazu gegeben zu haben.

> ? ***Schengenraum***
>
> *Der Schengenraum umfaßt derzeit folgende Staaten:*
> *Belgien,*
> *Deutschland,*
> *Frankreich,*
> *Griechenland,*
> *Italien,*
> *Luxemburg,*
> *Niederlande,*
> *Österreich,*
> *Portugal und*
> *Spanien.*
> *Demnächst auch:*
> *Dänemark*

- Auch die weitergehenden Auswirkungen der anlaßfreien Kontrolle müssen im Auge behalten werden. De facto führte sie zu der bisher nicht bestehenden Pflicht, ein **Identitätspapier** bei sich zu führen. Die Identitätsfeststellung macht überdies nur dann Sinn, wenn die festgestellten Personalien mit den polizeilichen Dateien abgeglichen werden. Nach den gesetzlichen Vorschriften über sog. Kontrollmeldungen kann es dabei auch zu Speicherungen solcher Personen kommen, die selbst polizeilich völlig unauffällig sind, sich jedoch in Gesellschaft der „falschen" Reisebegleiter befinden.
- Schließlich ist zweifelhaft, ob eine Personenkontrolle in einem definierten Streifen hinter den Schengengrenzen bzw. auf Durchfahrtsstraßen nicht einen Verstoß gegen das Schengener Durchführungsübereinkommen und den **„Geist von Schengen"** ist. Der freie Personenverkehr über die Schengengrenzen dürfte kaum damit in Einklang zu bringen sein, daß kurz hinter der Grenze umfangreiche Kontrollen stattfinden.

Aufgrund der weitreichenden Konsequenzen für die einzelnen Betroffenen und des eher zweifelhaften Nutzens halten wir im Ergebnis die Einführung der Schleierfahndung für **nicht verhältnismäßig** und damit für verfassungsrechtlich bedenklich.

Die Diskussion über die Schleierfahndung zeigt eines sehr deutlich: Nach bisherigem Recht muß der Bürger dem Staat einen Anlaß dafür geliefert haben, daß mit polizeilichen Mitteln gegen ihn vorgegangen werden kann. Die Einführung der anlaßfreien Identitätskontrolle würde diesen Grundsatz aushöhlen. Das Prinzip, wonach der Staat dem einzelnen Bürger den Grund dafür nachzuweisen hat, weshalb er polizeilichen Maßnahmen unterworfen wird, würde sich umkehren.

Jeder Bürger wäre zunächst potentiell verdächtig und hätte seinerseits das Gegenteil zu beweisen.

Was ist zu tun?
Es muß auch und gerade im zusammenwachsenden Europa dabei bleiben, daß Bürger von der Polizei nur dann kontrolliert werden dürfen, wenn ein konkreter Anlaß vorliegt.

4.2.6 Mit Videoüberwachung gegen Punker

Auf Sylt wird mit Videotechnik gegen Punker vorgegangen. Hierdurch sollen die Kurgäste vor Belästigungen geschützt und ein Rückgang der Kriminalität erreicht werden.

Seit 1996 wird in der Fußgängerzone von Westerland auf der Insel Sylt jeweils in der Hauptsaison auf dem Dach eines Geschäftshauses eine Videokamera installiert, um von dort aus das Geschehen im Bereich der Springbrunnenanlage aufzunehmen. Die Kamera ist nicht schwenkbar und über Funk verbunden mit der Wache der Polizeistation, wo die Bilder auf einem Monitor zu sehen sind. Im Einzelfall wird von der Möglichkeit des **Heranzoomens** von bestimmten Personen Gebrauch gemacht, wenn Vorgänge zu beobachten sind, die auf die Begehung von Straftaten hindeuten. Bildaufzeichnungen finden dagegen nicht statt. Begonnen wurde damit im Jahr 1995, als sich dieser Platz zu einem Treffpunkt für Punks entwickelte, die dort übernachteten, Alkohol konsumierten, Störungen verursachten und im Zusammenhang mit dem Alkoholkonsum auch Straftaten begingen.

Die Rechtsgrundlage für das Vorgehen findet sich im Landesverwaltungsgesetz. Danach dürfen allgemein zugängliche Flächen und Räume mittels **Bildübertragung** beobachtet werden, soweit dies zur polizeilichen Aufgabenerfüllung erforderlich ist. Aufzeichnungen sind zulässig, wenn im Einzelfall Tatsachen für die Begehung von schwerwiegenden Straftaten sprechen.

Diese gesetzlichen Vorgaben werden nach unseren Feststellungen eingehalten. Die Durchführung von Videoüberwachungen stellt allerdings einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Deshalb ist darauf zu achten, daß die Maßnahme nur solange fortgesetzt wird, wie in dem Bereich Störungen zu verzeichnen sind.

Was ist zu tun?
Die Videoüberwachung öffentlicher Plätze darf nicht zur Dauereinrichtung werden. Es muß deshalb stets geprüft werden, ob sie noch gerechtfertigt ist.

4.2.7 Videoeinsatz im Strafverfahren

Die Vernehmung von Opfern als Zeugen in einem Strafverfahren stellt z. B. in Fällen des sexuellen Mißbrauchs oftmals eine erhebliche Belastung dar. Diese Problematik ist in der letzten Zeit verstärkt in den Blickpunkt der öffentlichen Diskussion gerückt. Der Einsatz von Videotechnik kann eine Lösung bieten, wenn bestimmte Vorgaben beachtet werden.

Von seiten des Bundesrates sowie der Fraktionen der CDU/CSU und der F.D.P. wurden Gesetzesentwürfe eingebracht, die einen besseren Zeugenschutz durch den Einsatz von Videotechnik beabsichtigen. Dabei werden auch datenschutzrechtliche Fragestellungen berührt. Die Gesetzentwürfe sehen im wesentlichen zwei Maßnahmen vor:

- Bild-Ton-Direktübertragungen der Vernehmung aus einem anderen Raum in den Verhandlungssaal (sogenanntes „Mainzer Modell") und
- Bild-Ton-Aufzeichnungen richterlicher Vernehmungen im Ermittlungsverfahren als Beweismittel in der Hauptverhandlung zur Vermeidung einer Wiederholung der Vernehmungssituation

In einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder zu diesen Regelungen Stellung bezogen und empfohlen, die vorgesehenen Maßnahmen in einem umfassenderen Bedeutungs- und Funktionszusammenhang zu diskutieren. Bild-Ton-Aufzeichnungen sollen nämlich immer häufiger auch mit anderer Zielsetzung verwertet werden, z. B. um den Beweiswert einer Aussage zu verbessern.

Zu berücksichtigen ist dabei, daß die Aufzeichnungen einen erheblichen Eingriff in das **Persönlichkeitsrecht** darstellen, da sie die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend widerspiegeln. Aus diesen Gründen regen die Datenschutzbeauftragten die folgenden Vorkehrungen zum Schutz der Betroffenen an:

- Unverzichtbare Voraussetzung für das Vorgehen ist eine **Einwilligung** des Betroffenen bzw. seines Vertreters.
- Der Eindruck des Aussagegeschehens darf nicht – z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild oder Zoom – gezielt **verfremdet** oder **verzerrt** werden.
- Die gesetzlichen **Zeugnisverweigerungsrechte** müssen gewahrt bleiben, so daß insbesondere eine weitere Nutzung der Aufnahme auszuschließen ist, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
- Es müssen wirksame **Vorkehrungen** gegen einen **Mißbrauch** der Videokopien etwa durch Veröffentlichung in den Medien getroffen werden.
- Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die **Zwecke** dieses anderen Verfahrens

hätten angefertigt werden dürfen.

- Die **Verwendung** in **anderen** gerichtlichen **Verfahren** – etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht – ist unter engen und präzisen Voraussetzungen zu regeln.
- Es müssen eindeutige Bestimmungen über die weitere **Aufbewahrung** bzw. **Löschung** der Aufzeichnungen aufgenommen werden.

Was ist zu tun?
Der Gesetzgeber sollte bei der Regelung des Videoeinsatzes in Strafverfahren die o. a. Punkte berücksichtigen.

4.2.8 Privat-Fahndung im Internet

In der Informationsgesellschaft wird das kommerzielle Angebot von Informationen zu einem gewinnbringenden Geschäftszweig. Auch im Bereich innere Sicherheit kann man Geld verdienen. Beide Tendenzen treffen sich in einem neuartigen Informationsangebot im Internet, das wir zum Anfang des Jahres 1997 zu begutachten hatten.

Das „Europäische Sicherheits-Informationssystem" (**EuSIS**) eines Unternehmens aus Schleswig-Holstein zielt darauf ab, eine Informationsplattform für die private Sicherheitsbranche, aber auch für staatliche Strafverfolgungsbehörden herzustellen. Es bietet den im Bereich Sicherheit engagierten Unternehmen z. B. die Möglichkeit, ihre Dienstleistungen oder Technik und Literatur zum Thema zu offerieren. Aus datenschutzrechtlicher Sicht von Interesse ist vor allem die Absicht, in EuSIS gezielte **Fahndungsaufrufe** einzustellen. Wegen dieser Möglichkeit kam es zu verschiedenen Anfragen schleswig-holsteinischer Behörden an uns, die an der Rechtmäßigkeit des Angebots zweifelten. Unabhängig davon setzten sich auch die Betreiber von EuSIS mit uns in Verbindung, um die datenschutzrechtliche Zulässigkeit ihres Angebots prüfen zu lassen. Die Fahndungsmöglichkeiten in EuSIS teilen sich in drei verschiedene Kategorien: Personen-, Sach- und Ereignisfahndungen.

In die **Sachfahndung** werden vor allem gestohlene Gegenstände aufgenommen. Dies geschieht regelmäßig auf Veranlassung des Geschädigten. Soweit personenbezogene Daten einfließen, wird die Einwilligung des Betroffenen verlangt. Im Bereich **Ereignisfahndung** werden bestimmte Ereignisse, wie z. B. Straftaten, die bereits begangen wurden, beschrieben. Ziel der Ausschreibung ist hier, Hinweise auf noch unbekannte Täter zu erhalten. Dabei werden regelmäßig keine personenbezogenen Daten veröffentlicht. Soweit es um die personenbezogenen Daten der Geschädigten geht, soll auch hier deren Einverständnis der Geschädigten eingeholt werden.

Kritisch zu sehen ist vor allem der Bereich der sogenannten **Personenfahndung**. Nach dem Konzept von EuSIS sollte hier die Fahndung nach gesuchten Personen

4.2.7 Videoeinsatz im Strafverfahren

Die Vernehmung von Opfern als Zeugen in einem Strafverfahren stellt z. B. in Fällen des sexuellen Mißbrauchs oftmals eine erhebliche Belastung dar. Diese Problematik ist in der letzten Zeit verstärkt in den Blickpunkt der öffentlichen Diskussion gerückt. Der Einsatz von Videotechnik kann eine Lösung bieten, wenn bestimmte Vorgaben beachtet werden.

Von seiten des Bundesrates sowie der Fraktionen der CDU/CSU und der F.D.P. wurden Gesetzesentwürfe eingebracht, die einen besseren Zeugenschutz durch den Einsatz von Videotechnik beabsichtigen. Dabei werden auch datenschutzrechtliche Fragestellungen berührt. Die Gesetzentwürfe sehen im wesentlichen zwei Maßnahmen vor:

- Bild-Ton-Direktübertragungen der Vernehmung aus einem anderen Raum in den Verhandlungssaal (sogenanntes „Mainzer Modell") und
- Bild-Ton-Aufzeichnungen richterlicher Vernehmungen im Ermittlungsverfahren als Beweismittel in der Hauptverhandlung zur Vermeidung einer Wiederholung der Vernehmungssituation

In einer Entschließung haben die Datenschutzbeauftragten des Bundes und der Länder zu diesen Regelungen Stellung bezogen und empfohlen, die vorgesehenen Maßnahmen in einem umfassenderen Bedeutungs- und Funktionszusammenhang zu diskutieren. Bild-Ton-Aufzeichnungen sollen nämlich immer häufiger auch mit anderer Zielsetzung verwertet werden, z. B. um den Beweiswert einer Aussage zu verbessern.

Zu berücksichtigen ist dabei, daß die Aufzeichnungen einen erheblichen Eingriff in das **Persönlichkeitsrecht** darstellen, da sie die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend widerspiegeln. Aus diesen Gründen regen die Datenschutzbeauftragten die folgenden Vorkehrungen zum Schutz der Betroffenen an:

- Unverzichtbare Voraussetzung für das Vorgehen ist eine **Einwilligung** des Betroffenen bzw. seines Vertreters.
- Der Eindruck des Aussagegeschehens darf nicht – z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild oder Zoom – gezielt **verfremdet** oder **verzerrt** werden.
- Die gesetzlichen **Zeugnisverweigerungsrechte** müssen gewahrt bleiben, so daß insbesondere eine weitere Nutzung der Aufnahme auszuschließen ist, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.
- Es müssen wirksame **Vorkehrungen** gegen einen **Mißbrauch** der Videokopien etwa durch Veröffentlichung in den Medien getroffen werden.
- Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die **Zwecke** dieses anderen Verfahrens

4.2.9 Verkehrstätigkeitsbücher

Bei der Polizei werden Verkehrstätigkeitsbücher zu statistischen Zwecken geführt. Es wird aber auch eingetragen, wer einen bestimmten Verstoß begangen hat. Dies ist mit dem Zweck der Unterlagen nicht zu vereinbaren.

Durch eine Eingabe eines Polizeibeamten wurden wir darauf aufmerksam gemacht, daß in den sogenannten **Verkehrstätigkeitsbüchern** der Polizei auch personenbezogene Daten eingetragen werden. Es handelt sich hierbei um die Kfz-Kennzeichen und die Namen der Betroffenen.

Nach den Dienstanweisungen sollen die Unterlagen geführt werden, um eine „buchmäßige Kontrolle und statistische Auswertung aller Sachverhalte, Vorgänge und Maßnahmen zu ermöglichen". Für diese Zwecke wäre eine **anonymisierte Eintragung ausreichend**. Es ist nicht erforderlich, daß Polizeibeamte, die mit der konkreten Bearbeitung des Vorgangs nicht befaßt sind, über eine Einsichtnahme in das Verkehrstätigkeitsbuch erfahren, wer einen bestimmten Verkehrsverstoß begangen hat.

Demgegenüber beruft sich das Innenministerium bislang darauf, ohne eine Eintragung der personenbezogenen Angaben könnte den Betroffenen keine Auskunft über die Bearbeitung der Angelegenheit erteilt werden, da eine Zuordnung nicht möglich sei. Dies überzeugt nicht. Denn sofern ein verkehrsrechtlicher Verstoß vorliegt, wird ohnehin ein Vorgang angelegt, der in das neben dem Verkehrstätigkeitsbuch geführte **Ordnungsbuch** einzutragen ist, so daß auf diesem Wege die Zuordnung erfolgt. Bei verkehrsrechtlichen Sachverhalten, die keine weitere Bearbeitung erfordern, ist dagegen keine Konstellation zu erkennen, bei der im nachhinein personenbezogene Auskünfte aus den Verkehrstätigkeitsbüchern erteilt werden müssen. Dies wird dadurch bestätigt, daß in einigen Polizeirevieren auf die Eintragung personenbezogener Angaben in das Verkehrstätigkeitsbuch vollständig verzichtet wird. Nach unserer Auffassung liegt in den anderen Fällen eine nicht erforderliche Doppelerfassung vor, die das Risiko der Kenntnisnahme durch Unbefugte unnötig erhöht.

Was ist zu tun?
Der Innenminister sollte dafür sorgen, daß Verkehrstätigkeitsbücher in allen Polizeirevieren anonymisiert zu führen sind.

durch Private möglich sein. Rechtlich nachvollziehbar ist dies, soweit es um vermißte Minderjährige geht. In diesen Fällen reicht die Einwilligung der Eltern aus, um die Daten der Minderjährigen ins Internet einzustellen. Schon kritischer liegt die Sache, wenn es um vermißte Erwachsene geht. Wie die Erfahrung lehrt, kann hier nicht immer davon ausgegangen werden, daß die Vermißten einer Straftat zum Opfer gefallen sind. Nicht selten lösen sie sich vielmehr bewußt aus ihren Lebenszusammenhängen und „tauchen unter". Damit verwirken sie jedoch nicht das Recht, grundsätzlich selbst darüber zu bestimmen, ob sie im Internet gegebenenfalls mit Foto und Namensnennung auftauchen. Bei der Suche nach Volljährigen verlangen die Betreiber von EuSIS, daß die „Zustimmung" der Strafverfolgungsbehörden vorliegt. Diese Formulierung ist rechtlich bedenklich, führt jedoch bislang offenbar nicht zu rechtswidrigen Ergebnissen.

Die **Öffentlichkeitsfahndung nach Verdächtigen im Internet** kann grundsätzlich nur durch Strafverfolgungsbehörden, niemals durch Private veranlaßt werden. Rechtsgrundlage ist dafür § 131 StPO. Diese Vorschrift sieht allerdings nur den Erlaß eines sogenannten Steckbriefes vor und nicht eine irgendwie geartete Zustimmung der Strafverfolgungsbehörden zu Aktivitäten privater Dritter. In der Praxis kann es solange nicht zu Verstößen gegen die StPO kommen, wie die Strafverfolgungsbehörden nicht die „Zustimmung" zu irgendwelchen Ersuchen Privater erteilen. Das System EuSIS beinhaltete im Dezember 1997 lediglich eine Personenfahndung, die sich in ähnlicher Weise auch auf der Homepage des LKA Bayern wiederfand. In diesem Fall lag offenbar ein Steckbrief im Sinne der StPO vor.

Entscheiden sich die Strafverfolgungsbehörden, einen Beschuldigten mit Hilfe des Internets zu suchen, und liegen die oben aufgezählten Voraussetzungen vor, so ist es grundsätzlich unerheblich, ob die Ausschreibung auf der eigenen Homepage z. B. des LKA erfolgt oder ob sich die Strafverfolgungsbehörden dafür eines privaten Dienstleisters bedienen. Im zweiten Fall handelt es sich der Sache nach um **Auftragsdatenverarbeitung**. Dies verpflichtet die Strafverfolgungsbehörden u. a. dazu, sehr genau auszuwählen, wer mit einer solchen Aufgabe beauftragt wird. Von einer Zusammenarbeit der Strafverfolgungsbehörden in Schleswig-Holstein mit den Betreibern von EuSIS war zum Berichtszeitpunkt nichts bekannt.

Was ist zu tun?
Die Strafverfolgungsbehörden in Schleswig-Holstein müssen genau prüfen, ob sie mit privaten Internet-Providern zusammenarbeiten. Die Anbieter derartiger Dienste dürfen nicht alleine auf Ersuchen Privater sogenannte Fahndungsaufrufe veröffentlichen.

4.3 Verfassungsschutz

4.3.1 Beobachtung von Sekten?

Der Landtag debattiert eine Änderung des Verfassungsschutzgesetzes, um eine Beobachtung der Scientologen durch den Verfassungsschutz zu ermöglichen. Dadurch würde das Gesetz entscheidend verwässert.

Großes Aufsehen hat der Beschluß der Innenministerkonferenz des Bundes und der Länder erregt, die **Scientology-Organisation** vom Verfassungsschutz observieren zu lassen. Schleswig-Holstein ist das einzige Bundesland, das diesen Beschluß bislang nicht umgesetzt hat. Der Grund dafür ist eine Bestimmung im Landesverfassungsschutzgesetz. Diese besagt, daß eine Beobachtung von Organisationen durch den Verfassungsschutz deren „aktiv kämpferische, aggressive Haltung" gegenüber der bestehenden Verfassungsordnung voraussetzt. Das Erfordernis kann nach Auffassung des Innenministeriums bei den Scientologen derzeit nicht bejaht werden.

Um eine Beobachtung zu ermöglichen, wurde im Landtag ein Gesetzesantrag eingereicht, der eine ersatzlose Streichung der **„Aggressionsklausel"** vorsieht. Das hätte jedoch zur Folge, daß die Tätigkeit des Verfassungsschutzes auch in anderen Fällen uferlos ausgedehnt werden könnte. Im äußersten Fall wäre bereits eine gegen die freiheitlich-demokratische Grundordnung gerichtete Meinungsäußerung ein „Beobachtungsgegenstand". Alles, was der gewaltlosen politischen Meinungsfreiheit zuzurechnen ist, sollte aber in einem demokratischen Rechtsstaat von Überwachungsmaßnahmen ausgenommen sein. Wir haben uns deshalb gegen eine Änderung des Verfassungsschutzgesetzes ausgesprochen.

Was ist zu tun?
Die klaren Regelungen des Verfassungsschutzgesetzes des Landes Schleswig-Holstein sollten nicht aufgeweicht werden, nur um für den speziellen Fall der Scientologen eine Beobachtung durch den Verfassungsschutz zu ermöglichen.

4.3.2 Sicherheitsüberprüfungsgesetz längst überfällig

Seit Jahren drängen wir den Innenminister, endlich eine gesetzliche Grundlage für die bei einer Vielzahl von Personen im Lande vorgenommenen Sicherheitsüberprüfungen zu schaffen. Über mehrfache Ankündigungen, demnächst werde ein Entwurf vorgelegt, ist man bislang jedoch nicht hinausgekommen.

Ständig werden eine erhebliche Anzahl von Personen, die in Behörden, aber auch in der Privatwirtschaft in sogenannten sicherheitsempfindlichen Bereichen tätig sind, einer Sicherheitsüberprüfung unterzogen. Dabei werden nicht nur Erkenntnisse über das **Privat- und Vorleben** der Betroffenen eingeholt, sondern es können auch Überprüfungen des Lebenspartners durchgeführt werden. Privatper-

4.2.10 Polizei in einigen Bereichen vorbildlich

Polizei und Datenschutz sind Themen, die häufig kontrovers diskutiert werden. Beispiele dafür finden sich auch in diesem Bericht. Die praktische Zusammenarbeit zwischen unserer Dienststelle und den Polizeibehörden im Lande läuft allerdings gut. In einigen Bereichen ist die Polizei inzwischen vorbildlich.

Nachdem im Landesbeamtengesetz die Vorschriften über die Bearbeitung von Personaldaten erheblich verbessert wurden (vgl. 18. TB, Tz. 4.11.6), steht nun in den Behörden die Bereinigung der Personalakten an. Der Innenminister hat für den Polizeibereich **Personalaktenführungsrichtlinien** erlassen. Zusätzlich wurden speziell ausgebildete Mitarbeiter im Rahmen der Innenrevision in die Personalverwaltungsstellen zur Beratung gesandt. Diese wurden von uns begleitet, so daß **Datenschutz und Innenrevision Hand in Hand** arbeiteten. Die bislang erzielten Verbesserungen in der polizeilichen Personalaktenführung lassen erwarten, daß die Praxis dort in absehbarer Zeit den Vorschriften entspricht und für andere Behörden vorbildlich ist.

Schon seit einigen Jahren bestehen bei den Polizeidirektionen sowie beim Landeskriminalamt Ansprechpartner für Fragen des Datenschutzes. Sie waren allerdings bislang zumeist auch für die Informationsverarbeitung selbst verantwortlich, die ein Datenschutzbeauftragter im eigentlichen Sinne gerade zu kontrollieren hätte. Mittlerweile gibt es jedoch bereits in drei Direktionen und beim Landeskriminalamt **hauptamtliche Datenschutzbeauftragte**, die zumeist unmittelbar dem Behördenleiter zugeordnet sind. In weiteren Direktionen ist die Einrichtung einer derartige Stabsfunktion in Vorbereitung. Die Zusammenarbeit dieser Datenschutzbeauftragten untereinander wie auch mit uns hat sich im vergangenen Jahr noch intensiviert, zumal drei von ihnen jeweils für ein Jahr zur Ausbildung in unsere Dienststelle abgeordnet waren.

Die Polizei hat mit der Bestellung dieser Datenschutzbeauftragten eine **beispielgebende Rolle** übernommen. Es ist nicht auszuschließen, daß die Einrichtung von behördlichen Datenschutzbeauftragten im Zuge der Umsetzung der EU-Datenschutzrichtlinie auch für andere Behörden verbindlich wird. Angesichts des stetigen Ausbaus der automatisierten Datenverarbeitung und der Vielfalt der begleitenden Rechtsvorschriften ist die Polizei gut beraten, in Gestalt der Datenschutzbeauftragten Experten zum Datenverarbeitungsrecht zu beschäftigen. Für die Bürgerinnen und Bürger hat dies den Vorteil, daß die polizeiliche Datenverarbeitung intern überprüft und gegebenenfalls korrigiert wird, ohne daß es immer erst der externen Kontrolle durch uns bedarf.

4.4 Justizverwaltung

4.4.1 MEGA/MESTA

Die Automatisierung bei der Justiz wird mit Nachdruck vorangetrieben. Die erforderlichen rechtlichen Rahmenbedingungen konnte der Justizminister aber immer noch nicht fertigstellen.

Im 19. Tätigkeitsbericht (Tz. 4.4.1) hatten wir darüber berichtet, wie sich aus dem ursprünglich lediglich als Pilotprojekt angelegten Einsatz des Systems MEGA bei einem Amtsgericht plötzlich der Echtbetrieb in acht Amtsgerichten entwickelte. Ende 1997 lief **MEGA** bereits in zwölf Amtsgerichten. Besonders bemängelt hatten wir, daß ein so wichtiges Verfahren weitgehend ungeregelt eingeführt wurde. Es fehlte an begleitenden Vorschriften, die Einzelheiten der Datenverarbeitung regeln und technische und organisatorische Vorgaben für das Verfahren MEGA machen.

> **?** ***MEGA***
>
> *MEGA ist die Abkürzung für **Mehr**länder-**Ge**richts-**A**utomation. So nennen die Bundesländer Brandenburg, Schleswig-Holstein und Thüringen ihr gemeinsam neu entwickeltes EDV-Verfahren 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 und schnellere Erledigung von Schreibarbeiten. Den Richtern sollen bessere Informationsmöglichkeiten (z. B. durch die Abfrage von juristischen Datenbanken) die Entscheidungsfindung erleichtern.*

Leider hat sich an dieser Situation bis zum Redaktionsschluß des Tätigkeitsberichtes nichts geändert. Zwar hatten wir mehrfach Gelegenheit, uns zum Entwurf einer Dienstanweisung des Justizministeriums zu äußern und unsererseits Vorschläge zu machen. Wegen der komplizierten Regelungsmaterie und der verschiedenen dabei zu beteiligenden Gremien (Personalrat, Richterrat etc.) kam es bisher aber nicht zu einem Beschluß über den sogenannten **Betriebserlaß**. Positiv hervorzuheben ist allerdings, daß er – wenn er denn in Kraft tritt – nicht nur für den Einsatz des Verfahrens MEGA in den Gerichten gelten wird, sondern für sämtliche automatisierten Verfahren in den Justizbehörden.

Auch über das Verfahren **MESTA** haben wir im letzten Tätigkeitsbericht (Tz. 4.4.2) berichtet. Über den Fortschritt der Konzeption waren wir recht gut und frühzeitig unterrichtet. Unsere Stellungnahmen wurden von der Lenkungsgruppe aufgenommen und diskutiert. Wir hatten – ebenso wie Vertreter der Datenschutzbehörden der anderen beteiligten Länder – Gelegenheit, vorzutragen, welche Anforderungen aus datenschutzrechtlicher Sicht an das Verfahren zu stellen sind.

Nachdem in den übrigen beteiligten Bundesländern die Pilotphase von MESTA bei jeweils einer Staatsanwaltschaft bereits im Jahr 1997 startete, hat auch in

sonen – etwa Bekannte, Freunde, Kollegen etc. – können über den Betroffenen befragt werden. Prüfungen von Datenschutzbeauftragten in Akten des Verfassungsschutzes haben bundesweit ergeben, daß es dabei oftmals zu weit in die Persönlichkeitsphäre der Betroffenen hineinreichenden Datenerhebungen und -speicherungen kommt. Das Ergebnis der Sicherheitsüberprüfung ist oft von großer beruflicher Tragweite für den Betroffenen.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 kann kein Zweifel mehr daran bestehen, daß in diesem für das Persönlichkeitsrecht besonders empfindlichen Bereich eine gesetzliche Grundlage zu schaffen ist. 1988 erließ der Innenminister die „Sicherheitsrichtlinien" in Form einer einfachen Verwaltungsvorschrift, die auch heute noch Grundlage der Sicherheitsüberprüfung sind. Mit großer Verzögerung verabschiedete endlich der Bundesgesetzgeber 1994 für den Bereich der Bundesbehörden ein **Sicherheitsüberprüfungsgesetz**, dem bislang bereits einige Landessicherheitsüberprüfungsgesetze nachfolgten. Hierin hätte der Innenminister zumindest eine Orientierung für die Schaffung eines eigenen Entwurfs finden können. Trotz kontinuierlicher Nachfragen werden wir seit nunmehr drei Jahren mit dem Hinweis **vertröstet**, ein Entwurf befinde sich beim Innenminister in der hausinternen Abstimmung. Darüber hinaus ist jedoch, soweit für uns sichtbar, nichts geschehen.

Von anderer Seite kam jetzt allerdings Bewegung in die Sache, als sich im Berichtsjahr ein **Polizeibeamter** an uns wandte, der sich gegen seine beabsichtigte Sicherheitsüberprüfung zur Wehr setzen wollte. Er hat selbst tagtäglich die für die Polizei geltenden datenschutzrechtlichen Vorschriften bei seiner Arbeit zu beachten und konnte deshalb nicht einsehen, warum ein derart tiefgreifender Eingriff in sein Persönlichkeitsrecht immer noch ohne gesetzgeberische Entscheidung stattfinden sollte. Vor dem Verwaltungsgericht hätte er nach unserer Einschätzung gute Chancen gehabt. Der Innenminister hat die Brisanz der Lage nun offensichtlich erkannt und die Sicherheitsüberprüfung in Bezug auf den Petenten sowie für alle anderen Polizeibeamten auf vergleichbaren Dienstposten bis zur Schaffung einer gesetzlichen Grundlage zurückgestellt.

Es ist dringend erforderlich, daß nunmehr endlich ein Gesetzentwurf ausgearbeitet wird und alsbald ins Gesetzgebungsverfahren geht. Weitere Verzögerungen sind nicht länger hinnehmbar.

Was ist zu tun?
Der Innenminister muß schleunigst einen Gesetzentwurf für Sicherheitsüberprüfungen vorlegen.

gung von Daten öffentlicher Stellen entwickelt. Auch die Frage der **Protokollierung** der Datenabfragen ist nicht zu unserer vollständigen Zufriedenheit geklärt worden. Zwar werden die schreibenden Zugriffe vollständig protokolliert. Eine Protokollierung der nur lesenden Zugriffe (Abfragen) wird jedoch voraussichtlich nicht erfolgen, da dies angeblich die Systemressourcen zu stark beanspruchen und das Verfahren damit verlangsamen würde.

Was ist zu tun?
Der Betriebserlaß sollte so schnell wie möglich ergehen. Die noch offenen Fragen bei MESTA sollten vom Justizministerium und den einzelnen Staatsanwaltschaften weiterhin in Zusammenarbeit mit uns geklärt werden.

4.4.2 Informationsfluß beim Täter-Opfer-Ausgleich

Wenn Aufgaben, die bisher dem staatlichen Bereich zugeordnet waren, künftig von Privaten wahrgenommen werden, verschlechtert sich in aller Regel der datenschutzrechtliche Standard. Beim Täter-Opfer-Ausgleich wurden Sicherungen eingezogen, nachdem wir auf Bitten der Gerichtshelfer tätig wurden.

In einem Erlaß des Generalstaatsanwaltes aus dem Jahre 1996 wurde darauf hingewiesen, daß von der Möglichkeit des Täter-Opfer-Ausgleichs (TOA) verstärkt Gebrauch gemacht werden solle. Außerdem wurden dort Anwendungsfälle, Beteiligte und Verfahren des TOA festgelegt. Wegen des gesetzlich vorgeschriebenen Grundsatzes der Subsidiarität sollen bei der Durchführung des TOA vor allem die **freien Träger der Straffälligenhilfe** eingesetzt werden. Nur in wenigen Fällen werden noch die beim Land beschäftigten Gerichtshelfer selbst tätig. Die Einschaltung der freien Träger soll nach der Verfügung in der Weise erfolgen, daß die Staatsanwaltschaft „die notwendigen Informationen" an die freien Träger übermittelt. Ausdrücklich wurde darauf hingewiesen, daß eine Einverständniserklärung der Beteiligten für die Übermittlung nicht erforderlich sei. In der Praxis bedeutet dies, daß dieser strafgerichtlichen Akte von der Staatsanwaltschaft den freien Trägern ohne weitere Prüfung übermittelt wird.

> **?** ***Täter-Opfer-Ausgleich (TOA)***
> *Der TOA soll dazu dienen, einen Ausgleich des Unrechts einer Straftat zwischen dem Täter und dem Opfer herzustellen und zur Wiedergutmachung beizutragen. Der TOA wird nur durchgeführt, wenn sowohl Täter als auch Opfer damit einverstanden sind. In diesen Fällen wird unter Einschaltung einer dritten Stelle wie der Gerichtshilfe oder freier Träger versucht, einen konkreten Schaden, der beim Opfer noch vorliegt, durch den Täter ausgleichen zu lassen. Für den Täter kann dies dazu führen, daß seine Strafe gemildert oder ganz von der Strafe abgesehen wird.*

Das Problem besteht darin, daß das Datenschutzrecht, das für die freien Träger der Straffälligenhilfe gilt, weit unter dem Standard des Landesdatenschutzgesetzes

Schleswig-Holstein zum Jahreswechsel mit der **Pilotierung** bei der Staatsanwaltschaft Flensburg begonnen.

MESTA stellt gegenüber dem zur Zeit bei den Staatsanwaltschaften im Land eingesetzten Verfahren GAST eine **entscheidende Weiterentwicklung** dar. Neben dem aus GAST bekannten Informationssystem über Beschuldigten- und Verfahrensdaten (vgl. 18. TB, Tz. 4.4.1) sollen künftig auch die Vorgänge selbst mit EDV-Unterstützung bearbeitet werden. Dazu sind Standardsoftwareprodukte im Bereich der Textverarbeitung mit MESTA verknüpft. Für häufig vorkommende staatsanwaltschaftliche Schreiben werden Standardtexte aufgerufen, die fallspezifischen Daten werden unmittelbar aus der MESTA-Datenbank übernommen.

Als Rechtsgrundlage für MESTA besteht das **„Gesetz über die staatsanwaltschaftlichen Verfahrensregister"** (StARegG) vom Januar 1996 (vgl. 18. TB, Tz. 4.4.1). Dieses in der Bundesrepublik bislang einmalige Regelungswerk definiert den Umfang der Daten, die in die MESTA-Datenbank aufgenommen werden dürfen. Neben den Verfahrensdaten sind dies in der Regel nur die Daten der Beschuldigten, lediglich in Ausnahmefällen werden Personendaten der Geschädigten oder Anzeigenden gespeichert. Die Daten bleiben für zwei Jahre im landesweiten Zugriff, d. h. es kann von allen fünf Staatsanwaltschaften aus auf sie zugegriffen werden. Weitere drei Jahre sind die Daten lediglich im Zugriff der Staatsanwaltschaft, die sie eingespeichert hat. Danach dürfen die Daten nur noch verwendet werden, um die Akte oder einzelne Schriftstücke (z. B. Urteile), die nach wie vor in Papierform aufbewahrt werden, in der Registratur zu erschließen. Eine **Errichtungsanordnung** wurde zu Beginn der Pilotierung in Kraft gesetzt und regelt die Einzelheiten des Verfahrens.

? *MESTA*

*MESTA ist die Abkürzung für **Mehr**länder-**Sta**atsanwaltschafts-**Auto**mation. Zu diesem Projekt hatten sich ursprünglich die Länder Brandenburg, Hamburg und Schleswig-Holstein zusammengefunden und der Datenzentrale Schleswig-Holstein den Auftrag zur Entwicklung des Programms gegeben. Nachträglich ist noch das Land Hessen dem Vertrag beigetreten. Oberstes Leitungsgremium des Projektes ist die sogenann-te Lenkungsgruppe. Ihr gehören je ein Vertreter der vier Landesjustizverwaltungen und der Datenzentrale an. Den Datenschutzbeauftragten der beteiligten Länder wurde ein Sitz mit beratender Funktion zur Verfügung gestellt.*

Trotzdem sind derzeit noch viele **Fragen offen**. So sollen die Berechtigungen der Bediensteten, auf bestimmte Datengruppen zuzugreifen, erst auf Ebene der einzelnen Staatsanwaltschaften festgelegt werden. Es wird darauf zu achten sein, daß die **Zugriffsbefugnisse** bei der Vorgangsbearbeitung streng an der jeweiligen Zuständigkeit orientiert vergeben werden. Gerade angesichts des großen Kreises künftiger Benutzer von MESTA muß die unbefugte Kenntnisnahme sensibler Strafverfahrensdaten sicher ausgeschlossen werden. Die von uns geforderte verschlüsselte Datenübermittlung zwischen den einzelnen Staatsanwaltschaften wird es jedenfalls in der Pilotierungsphase noch nicht geben. Zunächst soll abgewartet werden, ob das Land ein Gesamtkonzept für die **Datenverschlüsselung** bei der Übertra-

4.4.3 Umfang beglaubigter Ausfertigungen von Scheidungsurteilen

Werden Scheidungsurteile zur Vorlage bei anderen Stellen angefordert, reicht es in der Regel, wenn bloß der Urteilstenor von den Gerichten herausgegeben wird. So soll von jetzt ab verfahren werden, wenn nicht ausdrücklich das komplette Urteil beantragt wird.

Eine Petentin hatte bei dem Landgericht Kiel eine beglaubigte Fotokopie des Scheidungsurteils ihrer Mutter angefordert, um diese bei einem Bestattungsunternehmen vorzulegen. Hierfür wäre es ausreichend gewesen, lediglich den **Urteilstenor** weiterzuleiten, aus dem sich ergibt, wann die Ehe rechtskräftig geschieden wurde. Wahrscheinlich aufgrund eines Mißverständnisses zwischen der Petentin und dem zuständigen Beamten der Geschäftsstelle wurde jedoch eine Kopie des kompletten Urteils mit Schuldspruch, Anhörung der Zeugen usw. übersandt.

Das Landgericht Kiel berief sich in einer Stellungnahme darauf, daß es **Sache des Antragstellers** sei, ein verkürztes Scheidungsurteil zu beantragen, wenn lediglich der Urteilstenor gebraucht werde. Dagegen spricht jedoch, daß viele Bürger, die mit der Materie nicht so vertraut sind, an diese Möglichkeit zunächst gar nicht denken. Dabei benötigen die bearbeitenden Stellen ganz überwiegend lediglich den Urteilstenor. So werden Dritten sensible persönliche Sachverhalte offenbart, obwohl es hierfür keinerlei Notwendigkeit gibt.

Deshalb haben wir eine Änderung des Verfahrens angeregt und erreichen können, daß zukünftig das gesamte Urteil mit den Entscheidungsgründen nur dann übersandt wird, wenn dies ausdrücklich beantragt worden ist. Mit der Übersendung der **verkürzten Urteilsausfertigung** wird der Hinweis gegeben, daß auf Wunsch auch die vollständige Fassung erhältlich ist.

4.5 Umweltschutz

Wenn ein Klimaschutzfonds die Atmosphäre verdirbt

Die Werbeaktion des Klimaschutzfonds eines Kreises verstieß nicht gegen das Datenschutzrecht, wie viele Bürger zunächst vermuteten. Durch rechtzeitige Aufklärung wäre die verständliche Aufregung vermieden worden.

Eine Reihe von Einwohnern eines Kreises erhielt eines Tages einen Brief von einem Klimaschutzfonds. Der Briefkopf enthielt auch den Namen des Kreises. Man nahm Bezug auf den Stromverbrauch des einzelnen Empfängers und rechnete ihm vor, daß er bei dem vorgesehenen **Wegfall des Kohlepfennigs** einen bestimmten konkreten Betrag im Jahr einsparen würde. Er wurde gebeten, diesen Betrag für die Arbeit des Klimaschutzfonds zu spenden. Damit sollten Solaranlagen auf Schulen gefördert und die Schüler über die Verwendung erneuerbarer Energien unterrichtet werden. Unterschrieben war der Brief vom Landrat des Kreises.

bleibt. Es kommt lediglich der dritte Abschnitt des Bundesdatenschutzgesetzes zur Anwendung, der allgemein das Datenschutzrecht bei nichtöffentlichen Stellen regelt. Diese Art von **„Outsourcing"** darf jedoch nicht dazu führen, daß das Datenschutzniveau für die Betroffenen unzumutbar absinkt, wenn die Strafverfahrensakten von der Staatsanwaltschaft ohne weitere Sicherungsmaßnahmen an die freien Träger weitergegeben werden. Andererseits ist aus Sicht der mit dem TOA befaßten Stellen nachvollziehbar, daß eine vorherige **Einverständniserklärung** aller Beteiligten vor der Informationsübermittlung im Regelfall nur unter großem Aufwand eingeholt werden kann. In der Praxis würde die Einholung dieser Einverständniserklärung bereits darauf hinauslaufen, daß mit allen Beteiligten gesprochen und insoweit der TOA fast vorweggenommen wird.

Wir haben die Fragen zunächst mit dem Generalstaatsanwalt erörtert, der uns bei der Einschätzung der Problemlage grundsätzlich zustimmte. Mit dem Justizministerium, das für die Beauftragung der freien Träger bei der Durchführung des TOA zuständig ist, haben wir sodann folgendes Vorgehen vereinbart:

Die Gewährung von Finanzmitteln für die freien Träger erfolgt im Wege der Projektförderung. Dem **Förderbescheid** an die einzelnen geförderten freien Träger wird künftig eine Anlage beigefügt, die dem LDSG entsprechende Bestimmungen zum Datenschutz enthält und die von den freien Trägern zu beachten ist. Neben einem Hinweis auf die Vertraulichkeit und besondere Sensibilität der Daten und die strikte Zweckbindung ihrer Verarbeitung wird u. a. die Pflicht festgeschrieben, nach Durchführung eines TOA sämtliche Unterlagen zurückzugeben und alle Speicherungen zu löschen. Weiterhin wird der Projektträger verpflichtet, **Kontrollen** durch den Landesbeauftragten für den Datenschutz zuzulassen.

Somit ist sichergestellt, daß es in diesem sensiblen Bereich nicht zu einem unvertretbaren Risiko für die datenschutzrechtlichen Belange der Betroffenen kommt. Wir werden im Rahmen unserer Kapazitäten durch punktuelle Kontrollen nachprüfen, wie der Datenschutz bei den freien Trägern in der Praxis gehandhabt wird.

Was ist zu tun?
In Fällen wie diesen, in denen öffentliche Aufgaben an Private übertragen werden, sollten die öffentlichen Stellen auch bedenken, daß dies nicht zum Verlust der Rechte der Betroffenen führen darf. Gegebenenfalls ist zu überlegen, wie Private den datenschutzrechtlichen Regelungen des LDSG unterworfen werden können.

strafen sowie Verurteilungen nach Erwachsenenstrafrecht in der Fahrerlaubnisakte gespeichert waren. Sie lagen teilweise schon viele Jahre zurück, und die meisten Verurteilungen waren nicht mehr aus dem Bundeszentralregisterauszug ersichtlich. Im Verkehrszentralregister selbst waren nur noch wenige Eintragungen gespeichert. Die **Speicherung** der Vorverurteilungen in der Fahrerlaubnisakte war trotz Löschung in den Registern **zulässig**. Fahrerlaubnisbehörden dürfen nämlich nach dem Bundeszentralregistergesetz noch Informationen verwenden, die bereits in den Registern getilgt waren.

Zu beanstanden war aber, daß die Fahrerlaubnisbehörde entgegen bestehender Anweisungen des Verkehrsministeriums den **Petenten nicht** vor Übersendung der Unterlagen an das medizinisch-psychologische Institut **informiert** hat. Das Verkehrsministerium hatte im Jahre 1994 angeordnet, im Falle einer medizinisch-psychologischen Untersuchung dem Betroffenen die Möglichkeit einzuräumen, vor Übersendung der Unterlagen an die Gutachterstelle Einsicht zu nehmen. Diese Regelung macht die Datenübermittlung für den Betroffenen transparent und zwingt überdies die Behörde, bei Einwendungen des Betroffenen den Inhalt der Informationen noch einmal zu überprüfen. Den Hinweis auf diese Möglichkeit enthält ein Vordruck, der mit dem o. g. Erlaß verbindlich eingeführt wurde. Die Fahrerlaubnisbehörde hatte dem Petenten jedoch einen alten Vordruck vorgelegt, der diese Aufklärung nicht enthielt.

Zu beanstanden war auch, daß in den übersandten Urteilen **Daten Dritter**, z. B. der Mitangeklagten, enthalten waren. Diese hätten zumindest vor der Übermittlung gelöscht werden müssen.

Was ist zu tun?
Fahrerlaubnisbehörden müssen bei Führerscheinakten sehr sorgfältig prüfen, welche Informationen an andere Stellen weitergegeben werden dürfen. Vor ihrer Weitergabe an einen Gutachter ist dem Betroffenen Gelegenheit zur Stellungnahme zu geben.

4.6.2 Zu lange Aufbewahrung von Bußgeldakten

Automatisiert gespeicherte Bußgeldfälle werden nach Fristablauf umgehend in der EDV gelöscht, die papierenen Akten füllen aber weiterhin die Regale.

Wir haben in diesem Jahr mehrere Bußgeldstellen, die für die Ahndung von Verkehrsordnungswidrigkeiten zuständig sind, überprüft. Die meisten Bußgeldstellen haben mittlerweile **automatisierte Verfahren** eingeführt. Nach der Feststellung einer Ordnungswidrigkeit wird der Vorgang in die EDV eingegeben und dadurch eine Kette von Verarbeitungsschritten ausgelöst. Es wird automatisch der Kfz-Halter ermittelt, danach auf einem Formblatt entweder ein Verwarngeldangebot oder ein Anhörbogen ausgedruckt und automatisiert versandt. Der Computer überwacht den Zahlungseingang. Geht die Zahlung ein, wird dies bei der Bußgeldstelle angezeigt und der Fall in der EDV nach einer kurzen Frist

Die Betroffenen vermuteten eine unzulässige Datenübermittlung vom Versorgungsunternehmen an den Klimaschutzfonds und von diesem an den Kreis. Der Schlußsatz des Schreibens wurde unter diesen Umständen von vielen Petenten geradezu als Hohn verstanden: „Dieser Brief wurde im Zusammenarbeit zwischen Ihrem Versorgungsunternehmen und dem Klimaschutzfonds ... unter Wahrung Ihrer datenschutzrechtlichen Interessen erstellt."

Im Zuge unserer Nachforschungen stellte sich heraus, daß der **„Klimaschutzfonds"** ein gesonderter Bereich im Kreishaushalt war, aus dem „Maßnahmen für die Nutzung regenerativer Energien, rationeller Energieumwandlung und Energieeinsparung im Gebiet des Kreises ..." finanziert werden sollten. Der Kreis hatte die Werbeaktion zu dem Zweck initiiert, den Topf durch Spenden zu füllen. Da er die konkreten Verbrauchsdaten nicht kannte, bat er das Versorgungsunternehmen um Mithilfe. Er erstellte ein vorgefertigtes Blankoschreiben, das vom Landrat unterzeichnet wurde. Dieses Schreiben wurde vom Versorgungsunternehmen mit Anschrift, Anrede und Einsparungsbetrag ergänzt, die aus den Kundendaten bekannt waren. Die fertigen Schreiben wurden versandt, ohne daß der Kreis vom endgültigen Inhalt Kenntnis erhielt. Ein Verstoß gegen Datenschutzvorschriften konnte also nicht festgestellt werden, denn es hatte keine Datenübermittlung stattgefunden.

Also alles in Ordnung? Nein! Wesentlich für den Datenschutz und das Vertrauen der Bürger ist die Offenheit, mit der die Verwaltung ihnen gegenüber auftritt und das eigene Handeln **transparent** macht. Daran fehlte es hier. Unruhe und Unzufriedenheit bei den Betroffenen und unnötiger Arbeitsaufwand bei den beteiligten Stellen hätte vermieden werden können, wäre das Verfahren von vornherein klar dargestellt worden.

Was ist zu tun?
Ein Satz mehr an Erläuterungen kann häufig Mißtrauen und „Staatsverdrossenheit" entgegenwirken.

4.6 Wirtschaft, Technik und Verkehr

4.6.1 Strafurteile in der Führerscheinakte

Vor der Anfertigung medizinisch-psychologischer Gutachten wird dem Sachverständigen häufig vorab die Führerscheinakte übersandt. Dies ist aber nur zulässig, wenn der Betroffene davon zuvor unterrichtet worden ist.

Einem Petenten war die Fahrerlaubnis für eine längere Zeit entzogen worden. Nun beantragte er ihre Wiedererteilung. Die Führerscheinstelle ordnete eine **medizinisch-psychologische Untersuchung** an. Dabei bemerkte der Petent, daß der Psychologe Informationen über ihn vorliegen hatte, die seiner Meinung nach von der Fahrerlaubnisbehörde schon lange hätten gelöscht werden müssen. Bei der Prüfung des Falles stellten wir fest, daß neben Auszügen aus dem Verkehrszentralregister und dem Bundeszentralregister auch verschiedene Urteile mit Jugend-

Verkehrsverstoß verarbeiten, ist daher sehr gering. Im Land Schleswig-Holstein ist praktisch nur die Datenzentrale mit der automatisierten Aufbereitung der Verwaltungsverfahren befaßt. Unsere Überprüfung dort ergab jedoch keinen Hinweis auf Unregelmäßigkeiten. Auch eine Recherche des Bundesbeauftragten für den Datenschutz beim Kraftfahrt-Bundesamt, bei dem die Daten aller Kraftfahrzeughalter zentral gespeichert sind, verlief ergebnislos. Auch dort wurde versichert, die vorhandenen Datensicherungsmaßnahmen schlössen aus, daß Mitarbeiter der **niederländischen Firma** Daten „zugesteckt" haben könnten. Der niederländischen Datenschutzaufsichtsbehörde wurde von der besagten Firma versichert, sie habe alle Informationen aus der CD-ROM der Deutschen Telekom „Telefax-Buch für Deutschland" entnommen.

Was ist zu tun?
Im Rahmen unserer Möglichkeiten werden wir die Sache weiterhin im Auge behalten.

4.7 Sozialwesen

4.7.1 Laxer Umgang eines Vermieters mit Sozialdaten

Sozialämter müssen dafür Sorge tragen, daß aus Sozialhilfemitteln gewährte Mietkautionen an sie zurückfließen. Sie haben aber auch eine Mitverantwortung, daß Vermieter mit Sozialdaten ihrer Mieter sorgsam umgehen.

Ein Sozialamt hatte einer Hilfeempfängerin die **Mietkaution** darlehensweise aus Sozialhilfemitteln gestellt. Dem Vermieter teilte das Sozialamt schriftlich mit, daß die Mietkaution übernommen worden sei und bei Beendigung des Mietverhältnisses nur an die Behörde ausgezahlt werden dürfe. Zugleich wurde der Vermieter gebeten, das Sozialamt umgehend zu informieren, wenn die Mieterin aus der Wohnung ausziehe. Durch diese Mitteilungen fühlte sich die betreffende Mieterin diskriminiert, zumal der Vermieter mit dritten Personen über die Kautionsregelung und in diesem Zusammenhang über den Umstand gesprochen habe, daß sie **Sozialhilfe** bezog.

Die Information des Vermieters hinsichtlich des Darlehens und auch die Aufforderung, den Auszug der Mieterin zu melden, war zwar zur Aufgabenerfüllung des Sozialhilfeträgers erforderlich und damit zulässig. Wir haben dem Sozialamt jedoch dringend nahegelegt, Vermieter in derartigen Fällen auf ihre Pflicht zur **vertraulichen Behandlung** der offenen Sozialdaten nach dem Sozialgesetzbuch hinzuweisen.

Was ist zu tun?
Wenn Behörden dritten Personen Sozialdaten übermitteln, müssen sie deutlich auf deren Sensibilität und das Geheimhaltungsinteresse der Betroffenen hinweisen.

automatisch gelöscht. Es entsteht aber nach wie vor für jeden Einzelfall ein Aktenvorgang. Diese Bußgeldakten werden in den jeweiligen Bußgeldstellen unterschiedlich lange aufbewahrt.

Nach unserer Meinung kommt nach Rechtskraft der Entscheidung nur noch eine kurze Aufbewahrungsfrist in Betracht. Die Bußgeldstellen teilten unsere Auffassung, verwiesen aber auf die bestehenden Weisungen. Ein alter Erlaß des Verkehrsministeriums legte nämlich Fristen fest, die unseres Erachtens zu lang waren und überdies von manchen Bußgeldstellen nicht einmal eingehalten wurden.

Wir haben daraufhin gemeinsam mit dem Verkehrsministerium **neue Aufbewahrungsfristen** definiert, die im Regelfall zu einer Vernichtung der Bußgeldvorgänge nach Ablauf eines halben Jahres führen werden. Nur unter bestimmten Gesichtspunkten kann im Einzelfall eine dreijährige Aufbewahrungsfrist in Betracht kommen. Der Entwurf des neuen Erlasses des Ministeriums befindet sich zur Zeit in der Abstimmung.

Was ist zu tun?
Das Verkehrsministerium sollte die neuen Aufbewahrungsfristen für Bußgeldakten möglichst bald in Kraft setzen.

4.6.3 Werbung für Radarwarngeräte – alles nur Zufall?

Werbung für Radarwarngeräte in zeitlicher Nähe zu Bußgeldern für Geschwindigkeitsüberschreitungen erregten Argwohn. Die Nachprüfungen ergaben keine Anhaltspunkte für eine unzulässige Datenweitergabe.

Autofahrer und Verwaltungen wiesen uns wiederholt darauf hin, daß eine Firma mit Sitz in den Niederlanden Betroffenen per Telefax den Kauf eines Warngerätes anbot, mit dessen Hilfe es möglich sei, Geschwindigkeitskontrollen der Polizei frühzeitig festzustellen. Die Betroffenen waren deshalb von der **unaufgeforderten Werbesendung** aufgeschreckt, weil sie jeweils kurz zuvor bei einer Geschwindigkeitsmessung der Polizei „geblitzt" worden waren. Keiner mochte einen Zufall im Zusammentreffen von Verkehrsereignis und der Offerte der niederländischen Firma annehmen. Wir stellten fest, daß dieses „Phänomen" auch in anderen Bundesländern auftrat und die dortigen Datenschutzbeauftragten mittlerweile ebenfalls solche Fälle überprüften.

Die zeitliche Nähe zwischen Verkehrsverstoß und Übersendung der Telefaxwerbung ließ den Verdacht zu, daß hier womöglich Informationen aus öffentlichen Stellen, die mit der Verfolgung der Ordnungswidrigkeit befaßt waren, an die Firma geflossen sein könnten.

Verkehrsordnungswidrigkeiten werden in Schleswig-Holstein fast vollständig automatisiert geahndet. Die Zahl der Stellen, die die Informationen über den

Vorsicht zu genießen."

Das Sozialamt stützte sich auf eine **Erklärung im Sozialhilfeantrag**, wonach die Antragsteller im Rahmen ihrer Mitwirkungspflicht in die Speicherung und Verarbeitung der im Antrag erhobenen Daten einwilligen. Weiter war vom Antragsteller folgender Passus unterschrieben worden: „Mit der Übersendung der Sozialhilfeakte an einen anderen Sozialleistungsträger, bei dem der Inhalt der Akte zur weiteren Aufgabenerfüllung benötigt wird, bin ich einverstanden."

Die Übersendung einer **vollständigen Sozialhilfeakte** ist jedoch nur dann zulässig, wenn der neue Sozialhilfeträger sämtliche darin enthaltenen Informationen auch tatsächlich benötigt. Dies dürfte in der Praxis eher die Ausnahme sein. In der Regel benötigt bei Wohnsitzwechsel des Sozialhilfeempfängers der neue Sozialhilfeträger nur einige Daten, z. B. Angaben über bereits gewährte Bekleidungszuschüsse, um sicherzustellen, daß keine Doppelzahlungen erfolgen. Soweit der neue Sozialhilfeträger zur korrekten Bearbeitung des Antrages Informationen benötigt, hat er dies gegenüber dem bisherigen Sozialleistungsträger konkret darzulegen.

Auch die **pauschal** erteilte **Einwilligung** kann deshalb nicht die Übermittlung von Daten, die nicht für die Hilfeberechnung erforderlich sind, rechtfertigen.

Was ist zu tun?
Vor der Versendung kompletter Sozialhilfeakten an andere Leistungsträger ist zu prüfen, ob alle in der Akte enthaltenen Daten tatsächlich für die weitere Bearbeitung erforderlich sind. Nur die benötigten Informationen dürfen angefordert werden.

4.7.4 Keine Sozialdaten für den Amtsausschuß

Ein Amtsausschuß darf in seiner Funktion als Selbstverwaltungsorgan den Prüfungsbericht über ein Sozialamt nur einsehen, wenn dieser anonymisiert ist.

Ein **Amtsausschuß** hatte um Übersendung eines Prüfungsberichtes gebeten, den das Rechnungsprüfungsamt des Kreises über die Arbeitsweise des Sozialamtes der Amtsverwaltung angefertigt hatte. Dies führte zum Interessenkonflikt: Der Amtsausschuß als Selbstverwaltungsorgan benötigte den Bericht, um die Personalausstattung des Amtes beurteilen und in den Haushaltsberatungen berücksichtigen zu können. Andererseits erfüllt das Amt die Sozialhilfeangelegenheiten nur im Auftrag des Kreises nach dessen Weisung. Damit ist der Amtsvorsteher nicht befugt, personenbezogene Sozialdaten an den Amtsausschuß als einem Organ der kommunalen Selbstverwaltung zu übermitteln. Dieser Interessenwiderstreit kann allerdings leicht durch eine **Anonymisierung** der betreffenden Daten gelöst werden. Die Übermittlung des Prüfberichtes ohne personenbezogene Daten von Sozialhilfeempfängern ist datenschutzrechtlich unbedenklich.

4.7.2 Wenn das Sozialamt eine Blankovollmacht will

Das Sozialamt darf bei der Überprüfung der Einkommens- und Vermögensverhältnisse von Sozialhilfeempfängern nur dann eine Ermächtigung zur Einholung von Bankauskünften fordern, wenn konkrete Anhaltspunkte für falsche oder unvollständige Angaben des Hilfeempfängers vorliegen. Pauschale Ermächtigungsklauseln auf Überprüfungsbögen sind unzulässig.

Ein Bürger, der im Rahmen des Bezuges von Sozialhilfeleistungen dem Sozialamt gegenüber seine persönlichen und wirtschaftlichen Verhältnisse darlegen sollte, beschwerte sich bei uns über folgenden Passus des von ihm auszufüllenden und zu unterschreibenden **Überprüfungsbogens**: „Hiermit ermächtige ich außerdem alle Sparkassen und Banken, insbesondere die o. g. Banken und Geldinstitute, dem Kreissozialamt Auskunft über die Höhe aller Guthaben meiner jetzigen und früheren auf meinen Namen geführten Konten zu geben. Hierzu zählen auch unter Umständen die Konten, die als Gläubiger meinen Ehegatten ausweisen."



Die generelle und formularmäßige Aufforderung, der **Einholung von Bankauskünften** zuzustimmen, ist nicht von der Verpflichtung des Hilfeempfängers zur Angabe leistungserheblicher Tatsachen und der sonstigen Mitwirkungspflicht gedeckt. In erster Linie muß der Hilfeempfänger selbst seine Einkommens- und Vermögenssituation darlegen und die erforderlichen Nachweise beifügen. Das Sozialamt darf bei Dritten – d. h. auch bei Banken – nur dann nachfragen, wenn konkrete Zweifel an der Richtigkeit bzw. Vollständigkeit der Angaben bestehen. Diese Auffassung wird auch von der verwaltungsgerichtlichen Rechtsprechung vertreten. Das betreffende Sozialamt hat zugesagt, künftig die Einwilligung nur im konkreten Einzelfall einzuholen.

Was ist zu tun?
Überprüfungsbögen, in denen Sozialhilfeempfänger eine pauschale Auskunftsermächtigung erteilen müssen, dürfen von den Sozialämtern nicht mehr verwendet werden.

4.7.3 Akten von Hilfeempfängern dürfen nicht automatisch „mit umziehen"

Wird durch Wohnsitzwechsel eines Sozialhilfeempfängers ein anderer Sozialhilfeträger zuständig, so darf nicht routinemäßig die gesamte bestehende Sozialhilfeakte an die neu zuständige Stelle gesandt werden.

Anläßlich einer Prüfung in einem Sozialamt ergab sich, daß dort üblicherweise die gesamten Akten neu **zugezogener Sozialhilfeempfänger** vom zuvor zuständigen Sozialhilfeträger angefordert wurden. Aus den Akten wurden sodann die für die weitere Berechnung des Sozialhilfeanspruches relevanten Daten entnommen. Neben den für die Ermittlung des Hilfeanspruches tatsächlich erforderlichen Daten befanden sich in den Akten jedoch auch andere Angaben, die teilweise wertenden Charakter hatten. So stießen wir auf Bemerkungen wie: „Herr X ist mit

außerdem, daß die betreffenden technischen Dienstleister Patientendaten auf eigenen Sicherungskopien festhalten, z. B. um für den Fall (privat-)vertraglicher Auseinandersetzungen die Ordnungsmäßigkeit der erbrachten Dienstleistungen zu dokumentieren. All diese Personen sind **keine Ärzte** und daher zumindest nicht der berufsrechtlichen Schweigepflicht unterworfen. Außerdem sind Patientendaten in ihrer Obhut, anders als wenn sie sich bei Ärzten befinden, nicht gegen strafprozessuale Beschlagnahme geschützt.

Eine wirksame Einwilligung des Patienten in die Datenoffenbarung durch den Arzt an diese Personen, deren Zahl und Funktion er im Normalfall weder kennt noch abschätzen kann, ist hier kaum noch denkbar. Sie wäre so pauschal, daß sie zu einem bloßen Formalismus degradiert würde, der als rechtsverbindliche Willenserklärung nicht anerkannt werden könnte.

Die Fragen, die der verstärkte Einsatz von Informationstechnik im Gesundheitswesen aufwirft, waren Gegenstand der Sommerakademie 1997 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN, an der über 300 Ärzte, Juristen, Techniker und Datenschutzbeauftragte teilgenommen haben. Die Einzelheiten der Vorträge und Diskussionen sind in der Dokumentation der Veranstaltung nachzulesen. Folgende Gesichtspunkte spielten eine besondere Rolle:

- Jeder zusätzliche ärztliche Computereinsatz sollte gedanklich daraufhin überprüft werden, ob er für eine effektivere und bessere Behandlung tatsächlich **erforderlich** ist. Ein bloßer Einsatz zum „Selbstzweck" des technischen Fortschrittes rechtfertigt die Risiken unbefugter Datenoffenbarungen und Durchbrechungen der ärztlichen Schweigepflicht nicht.
- Auch die Technik selbst kann zur Lösung von Datenschutzproblemen beitragen. Wirksame Datensicherheitskonzepte unter Verwendung von **Verschlüsselungsverfahren** und **digitaler Signatur** können verhindern, daß technische Dienstleister auf sensible Daten zugreifen bzw. daß es zu Modifizierungen oder Verfälschungen kommt.
- Schließlich muß in einer faktisch (durch Technik) veränderten „ärztlichen Behandlungswelt" grundsätzlich über Sinn und Zweck **ärztlicher Dokumentationen** sowie über Ausgestaltung und Grenzen der ärztlichen Verschwiegenheitspflicht neu nachgedacht werden.

Die Diskussion über diese Fragen ist auch nach der Sommerakademie fortgeführt worden. In einer Reihe von Vorträgen haben wir unsere Vorstellungen präzisiert und vielen Zuhörern innerhalb und außerhalb Schleswig-Holsteins nähergebracht. Bei der Gesundheitsministerin ist dies auf fruchtbaren Boden gefallen. Sie hat angekündigt, das Land werde ein **Krankenhausdatenschutzgesetz** erlassen.

Was ist zu tun?
Wir werden uns auch künftig an der Diskussion über diese Fragen beteiligen und im Rahmen unserer Möglichkeiten Lösungskonzepte aktiv mitgestalten.

Was ist zu tun?
Durch Anonymisierung können häufig Interessenkonflikte bei der Bereitstellung von Informationen gelöst werden.

4.8 Gesundheitswesen

4.8.1 Computermedizin und Patientengeheimnis

Eine wichtige Entwicklung im Bereich des Gesundheitswesens ist die Zunahme der Computermedizin. Den damit für das Patientengeheimnis drohenden Risiken muß mit effektiven Maßnahmen begegnet werden.

Wie immer man den Begriff der Computermedizin auch definiert – sei es als Einsatz von Computertechnik im gesamten Gesundheitsbereich einschließlich verwaltender Tätigkeiten, sei es im engeren Sinne als Einsatz direkt im Behandlungsbereich: Stets wird durch „Zwischenschaltung" von Informationstechnik das traditionelle Verhältnis zwischen Arzt und Patient berührt. Dieses Verhältnis beruht auf der berufs- und strafrechtlich festgeschriebenen **Verschwiegenheitspflicht** des Arztes, und zwar grundsätzlich desjenigen Arztes, in dessen Behandlung sich der Patient begibt.

Das gilt im besonderem Maße auch für Behandlungen im **Krankenhaus**. Hier nimmt der Patient zwar regelmäßig eine „Kompaktleistung" aus ärztlichen und pflegerischen Tätigkeiten in Anspruch und vertraut sich somit all den Personen an, die im Rahmen einer ordnungsgemäßen und effektiven Behandlung unter verantwortlicher Leitung des behandelnden Arztes diese Gesamtleistung erbringen. Dabei kann auch die Zuziehung weiterer Ärzte erforderlich sein, denen dann Informationen über den betreffenden Patienten offenbart werden. Maßgeblich für die Befugnis, diese sensiblen Daten zu offenbaren, ist grundsätzlich die ausdrückliche Einwilligung des Patienten in Kenntnis aller Umstände. Auch kommt eine stillschweigende Einwilligung in Betracht, wenn der Patient sich wegen der Art seiner Erkrankung von vornherein darauf einstellt, daß eine ressortübergreifende Behandlung durch mehrere Fachärzte durchgeführt werden wird. Auch komplexe elektronische Krankenhausinformationssysteme müssen sich an diese Regeln halten.

Mit fortschreitender Computerisierung im ärztlichen Behandlungsbereich nimmt jedoch die Zahl von nichtbehandelnden Personen, die Zugriffsmöglichkeiten auf Patientendaten erhalten, deutlich zu. So sind in eine „telemedizinische" Behandlung von Patienten zahlreiche **externe Dienstleister** eingeschaltet, die sich mit der technischen Ermöglichung und Durchführung der Bild-, Ton- und sonstigen Dokumentenübertragungen befassen. Beispielsweise müssen die auf dem Übertragungsweg digitalisierten Daten für den jeweils angesprochenen Empfänger (Arzt) wieder lesbar gemacht werden. Auch gelangen die übertragenen Daten an den Übertragungsknotenpunkten der betreffenden Netze in den Verfügungsbereich Dritter, die zumindest die Möglichkeit der Kenntnisnahme haben. Denkbar ist

Ein Anspruch auf Löschung der Daten hätte in diesem Fall nur bestanden, wenn ihre Speicherung von vornherein unzulässig gewesen wäre; hätte es sich um **inhaltlich falsche** Daten gehandelt, wären diese zu berichtigen gewesen. Im Falle von ärztlichen Beurteilungen und Wertungen sind die Kriterien „zulässig", „unzulässig", „richtig" oder „falsch" nur begrenzt anwendbar. Eine **eigene Sachverhaltsdarstellung** des Patienten erschien uns deshalb als ein gangbarer Weg, um die Interessen aller Beteiligten zu wahren. Dies wurde von den behandelnden Ärzten offenbar ebenso gesehen: Auf unsere Nachfrage hin fanden sich alle angesprochenen Kliniken dazu bereit, die „Gegendarstellung" des Patienten der jeweiligen Krankenakte beizufügen.

Was ist zu tun?
Psychiatrische Kliniken sollten in vergleichbaren Fällen den Patienten ein Recht zur eigenen Sachverhaltsdarstellung geben.

4.8.3 Datenschutz bei der Schwangerschaftskonfliktberatung

Bei der Schwangerschaftskonfliktberatung geben die Betroffenen besonders intime Informationen über sich preis. Die Überprüfung einer Beratungsstelle ergab hinsichtlich des Umgangs mit diesen sensiblen Informationen erfreulicherweise keine Beanstandungen.

Im August 1995 ist das Schwangerschaftskonfliktgesetz in Kraft getreten. Es stellt detaillierte Anforderungen an die **Schwangerschaftskonfliktberatung**, die einem Schwangerschaftsabbruch vorausgehen muß, damit dieser straflos bleibt. In diesem sensiblen Bereich ist die Einhaltung der datenschutzrechtlichen Bestimmungen besonders bedeutsam. Die unbefugte Offenbarung von Daten betroffener Frauen durch Mitarbeiter der Beratungsstellen ist – wie die Offenbarung von Patientendaten durch Ärzte – nach § 203 Abs. 1 Strafgesetzbuch strafbar.

Unsere Überprüfung einer solchen Beratungsstelle erbrachte aus datenschutzrechtlicher Sicht ein erfreuliches Ergebnis: Die Vorschriften des **Schwangerschaftskonfliktgesetzes**, des Strafgesetzbuches sowie des Landesdatenschutzgesetzes wurden hier weitestgehend beachtet. Zu bemängeln war lediglich die Praxis eines Beraters, die Termine mit beratungssuchenden Frauen unter Namensnennung in seinem zwar nur von ihm geführten, jedoch auch privat genutzten Terminkalender zu notieren. Die Eintragungen erfolgen in Zukunft ohne Erwähnung der Namen.

> ? ***Schwangerschaftskonfliktgesetz***
>
> *Das Schwangerschaftskonfliktgesetz regelt u. a. die Schwangerschaftskonfliktberatung, die dem Strafgesetzbuch zufolge Voraussetzung für die Straflosigkeit eines Schwangerschaftsabbruches ist. Auf Wunsch kann die ratsuchende Frau anonym bleiben. Nach der Beratung wird eine Bescheinigung ausgestellt. Die Beratungsstellen ihrerseits erstatten ihrer Aufsichtsbehörde jährlich in anonymisierter Form Bericht über Maßstäbe und Erfahrungen der Beratungstätigkeit.*

4.8.2 „Gegendarstellung" in der psychiatrischen Krankenakte

Patienten haben ein Einsichtsrecht grundsätzlich auch in psychiatrische Behandlungsakten. Bei Meinungsunterschieden über die „Richtigkeit" des Akteninhalts kann eine eigene Sachverhaltsdarstellung des Patienten hilfreich sein.

Nach ständiger Rechtsprechung steht der ärztlichen Pflicht, über die Patientenbehandlung Aufzeichnungen zu führen, ein Recht des Patienten gegenüber, die in dieser Dokumentation enthaltenen sachlichen Befunde und Berichte einzusehen. Dieser Anspruch wird aus dem **Selbstbestimmungsrecht** und der personellen Würde des Patienten hergeleitet: Auch im Rahmen des Arztvertrages darf der Patient nicht zum bloßen Handlungsobjekt herabgewürdigt werden. Persönliche Eindrücke und Verdachtsdiagnosen des Arztes fallen jedoch nicht unter dieses Einsichtsrecht.

Besondere Bedeutung erlangt diese Einschränkung bei **psychiatrischen Krankenakten:** Hier sind die objektiven Befunde und Behandlungsfakten meist untrennbar vermengt mit Aufzeichnungen des Arztes über persönliche Eindrücke und Beurteilungen; typischerweise bilden diese sogar den Hauptgegenstand der Patientenakte. Neben dieser persönlichen Betroffenheit des Arztes sowie gegebenenfalls dritter Personen können überdies auch therapeutische Bedenken einer Offenlegung dieser ärztlichen Aufzeichnungen entgegenstehen. Ein Einsichts- bzw. Auskunftsrecht besteht hier demnach nur in **eingeschränkter Form**. Nimmt der Patient Einsicht oder erhält er ärztlicherseits Auskunft über den Inhalt der ihn betreffenden Unterlagen, kann es hinsichtlich der gespeicherten Informationen zu Meinungsverschiedenheiten kommen.

> **?** ***Patientenakte***
>
> *Gemäß § 15 der Ärztlichen Berufsordnung Schleswig-Holsteins ist der Arzt zu Aufzeichnungen über die in Ausübung seines Berufes getroffenen Feststellungen und Maßnahmen verpflichtet. Diese Aufzeichnungen sind sodann mindestens 10 Jahre aufzubewahren. Aus den Bestimmungen der Berufsordnung, der Judikatur zu den Rechten und Pflichten des Behandlungsvertrages sowie zum informationellen Selbstbestimmungsrecht ergibt sich, daß die Dokumentation nicht nur im Interesse des Arztes, sondern auch im Patienteninteresse erfolgt. Daraus hat die Rechtsprechung ein Einsichts- bzw. Auskunftsrecht des Patienten hinsichtlich objektiver physischer Befunde und Behandlungsverläufe abgeleitet.*

So wandte sich ein Bürger, der in verschiedenen psychiatrischen Kliniken behandelt worden war, an uns. Er machte geltend, sein Krankheitsbild und auch der Behandlungsverlauf seien in den ärztlichen Dokumentationen der Kliniken unrichtig wiedergegeben worden, und bat um Prüfung, ob die nach seiner Auffassung falschen Informationen gelöscht werden könnten. Zumindest wollte er eigene Sachverhaltsschilderungen zu den jeweiligen Krankenakten geben.

kenne. Die Lehrerin verwies jedoch darauf, daß ihre bei einem früheren Besuch im Kindergarten gemachten Beobachtungen durch das jetzige Verhalten des Kindes bestätigt würden. Der Vater hielt es für unzulässig, Verhaltensdaten von Kindergartenkindern zu erfassen und diese dann in der Schule weiter zu verwenden.

Es stellt sich die Frage, ob die Schule schon **Verhaltensbeobachtungen im Kindergarten** vornehmen darf, bevor die Kinder überhaupt in die Schule aufgenommen werden. Die Schule teilte uns dazu zunächst mit, es würden keine Verhaltensdaten im Kindergarten erhoben, sondern nur – wie auch vom Kindertagesstättengesetz zur Vorbereitung auf den schulischen Alltag gefordert – Kontakte zum Kindergarten gepflegt, um den schulpflichtig werdenden Kindern z. B. durch einen Tagesbesuch bei der zukünftigen Schule den Übergang zu erleichtern. Es mußte jedoch auf unsere Nachfrage eingeräumt werden, daß in diesem Falle wohl doch Verhaltensdaten im Kindergarten ermittelt wurden. Der Träger des kommunalen Kindergartens war der Auffassung, daß die Zulässigkeit sich bereits aus dem Zusammenarbeitsgebot des Kindertagesstättengesetzes ergebe.

Nach dem Schulgesetz ist vor der Einschulung eine **Schulreifeuntersuchung** durchzuführen, von deren Ergebnis die Schule unterrichtet wird. Der Schularzt stellt dabei fest, ob ein Kind aufgrund seiner Entwicklung in der Lage ist, den Anforderungen der Grundschule zu folgen, oder ob gegebenenfalls eine andere Schulform angeraten ist. Bei der Untersuchung soll zumindest ein Elternteil anwesend sein, sie erfolgt also mit Kenntnis der Erziehungsberechtigten. Auch die Ergebnisse eines etwaigen Schulreifetests müssen mit den Eltern besprochen werden. Diese Maßnahmen beginnen jedoch erst, wenn die Eltern aufgefordert werden, ihr Kind zur Schule anzumelden. Die Schule hat somit bis zur Einschulung des Kindes keine Berechtigung, Leistungs- oder Verhaltensdaten zu erheben.

Während unsere Rechtsauffassung bei der Schule auf wenig Gegenliebe stieß, hat der Träger des kommunalen Kindergartens reagiert. Er hat seine Mitarbeiterinnen und Mitarbeiter darauf hingewiesen, daß Verhaltens- und Leistungsdaten von Kindern nur mit **Einverständnis der Eltern** übermittelt werden dürfen.

Was ist zu tun?
Das Bildungsministerium sollte den Schulen gegenüber klarstellen, welche Informationen die Schulen für die Feststellung der Schulreife erhalten dürfen.

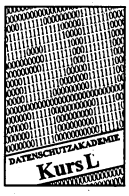
4.9 Kultusbereich

4.9.1 Wenn vertrauliche Papiere bei der Zeitung statt im Reißwolf landen

Ein Schulleiter beauftragte Schüler mit der Beseitigung von „Altpapier", das vertrauliche Daten enthielt. Durch eine Panne gelangten die Unterlagen an die Presse. Der Schulleiter machte die Erfahrung, wie Datenschutz blitzschnell „Chefsache" werden kann.

„Datenskandal an der Schule" lauteten die Schlagzeilen, die sogar zu einer Erörterung des Falles im Bildungsausschuß des Landtages führten. Was war geschehen? Eine Schule wollte Platz schaffen und hatte sorgsam getrennt: Eine Reihe von Kartons enthielt **Altpapier** und Pappe sowie unverfängliche Unterlagen ohne Personenbezug. Ein Karton war mit solchen Papieren gefüllt, die sorgsam vernichtet werden sollten; denn sie enthielten u. a. personenbezogene Daten aus **Schülerakten** wie Tadel, Entschuldigungsschreiben, Entwicklungsberichte, Protokolle von Elterngesprächen und ähnliches. Dieser Container war vor dem Schulsekretariat abgestellt worden und sollte in der Aktenvernichtungsanlage des Schulträgers entsorgt werden.

Der Schulleiter ließ nun eine Schulklasse das Altpapier in die entsprechenden Container der Müllabfuhr bringen. Ein Behälter konnte darin nicht mehr untergebracht werden und blieb auf der Straße stehen. Es war ausgerechnet der mit den **sensiblen Unterlagen**, den die Schülerinnen und Schüler versehentlich zusammen mit den anderen Kartons abtransportiert hatten. Passanten fanden die Papiere und leiteten einige der Unterlagen der Presse zu.



Wir haben diesen Vorfall als erheblichen Verstoß gegen Datenschutzvorschriften beanstandet, denn der Schulleiter hätte die Vernichtung der sensiblen Daten sorgsamer überwachen müssen.

Was ist zu tun?
Der Umgang mit sensiblen Verwaltungsunterlagen, und dazu gehört auch deren Vernichtung, ist sorgfältig zu organisieren und zu kontrollieren. Die Verantwortung dafür trägt der Behördenleiter.

4.9.2 Der kurze Draht zwischen Kindergarten und Schule

Auffälligkeiten von Kindern im Kindergarten dürfen der Schule nur unter bestimmten Voraussetzungen mitgeteilt werden.

Ein Kind besuchte die erste Klasse einer Grundschule und war wegen einer leichten Wahrnehmungsstörung nicht so leistungsfähig wie andere Kinder seiner Klasse. Die Klassenlehrerin, die den Unterricht der Klasse erst im Laufe des Schuljahres übernommen hatte, empfahl dem Vater deshalb den Wechsel in die Förderschule. Der Vater wandte ein, daß sie seinen Sohn doch erst seit kurzem

4.10 Steuerverwaltung

4.10.1 Wahrung des Steuergeheimnisses im Gemeinschaftsrechenzentrum

Bis zum letzten Moment ließ die Steuerverwaltung die Frage offen, ob nach der Bildung eines Gemeinschaftsrechenzentrums auch Mitarbeiter der Datenzentrale Einblick in Inhalte von Steuerbescheiden erhalten dürfen. Ein eindeutiges Votum des Finanzausschusses des Landtages hat offenbar dazu beigetragen, daß dem Steuergeheimnis der gleiche Stellenwert beigemessen wird wie in der Vergangenheit.

Im August 1977 sind das Rechenzentrum der Steuerverwaltung und das der Datenzentrale zusammengeführt worden, um ein wirtschaftlicheres Arbeiten als in der Vergangenheit zu ermöglichen. Diesem technisch anspruchsvollen Projekt sind intensive Beratungen in einer eigens eingerichteten Projektgruppe vorausgegangen. Wie im 19. Tätigkeitsbericht (Tz. 4.10.1) dargestellt, waren allerdings nicht nur technische, sondern auch rechtliche Probleme zu lösen. Eine dieser Fragen bezog sich auf das **Steuergeheimnis**. Die Steuerverwaltung neigte zunächst dazu, ihren bis dahin vertretenen Rechtsstandpunkt aufzugeben, wonach die strengen gesetzlichen Regelungen in der Abgabenordnung es ausschließen würden, daß externe Dienstleister (Auftragnehmer), die aus rein wirtschaftlichen Gründen eingeschaltet werden, personenbezogene steuerliche Daten zur Kenntnis nehmen dürfen.

Zu verlockend schienen die Einspareffekte, wenn Personalengpässe bei der Oberfinanzdirektion durch „Springer" der Datenzentrale ausgeglichen werden könnten. Wir haben stets vor einer solchen, juristisch nicht vertretbaren Auslegung der Bestimmungen über das Steuergeheimnis gewarnt, zu einer eindeutigen Positionsbestimmung in unserem Sinne war das Finanzministerium aber zunächst nicht zu bewegen.

Deshalb kam dem einstimmigen **Votum des Finanzausschusses** in seiner 34. Sitzung im Mai 1997, in dem festgestellt wurde, daß die „noch zu formulierenden Servicevereinbarungen im Rahmen des Projektes zur Integration der Rechenzentren von Landes- und Steuerverwaltung (PILS) sicherstellen müßten, daß die Mitarbeiter der Datenzentrale (DZ) die Inhalte steuerlicher Datenbestände und umgekehrt die Mitarbeiter der Oberfinanzdirektion (OFD) die Inhalte sonstiger Datenbestände nicht zur Kenntnis nehmen können", eine besondere Bedeutung zu.

> **?** ***PILS***
>
> *PILS steht für **P**rojekt zur **I**ntegration der Rechenzentren des **L**andes und der **S**teuerverwaltung. Die Zusammenlegung von zwei bisher getrennten Rechenzentren soll zu einer besseren Auslastung der technischen Systeme führen und damit Kosten sparen.*

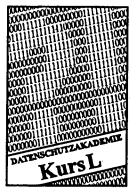
Wie „sensibel" dieser Punkt für die Steuerverwaltung und die DZ war, zeigte sich daran, daß das Problem ursprünglich in den **Service-Vereinbarungen** sibyllinisch

4.9.3 Ewiger Zankapfel: Unterrichtung der Elternvertreter

Immer wieder wehren sich einzelne Eltern dagegen, daß Elternbeiratsmitglieder Unterlagen über ihre Kinder einsehen. Bislang möchte das Kultusministerium keine Abhilfe schaffen.

Schon im 18. Tätigkeitsbericht (Tz. 4.9.5) sprachen wir es an: Es sind Fälle denkbar, in denen die berechtigten Interessen von Eltern oder Schülern eigentlich dazu zwingen, Mitgliedern der **Elternvertretung** Einsicht in Unterlagen von Einzelfällen zu verweigern, auch wenn z. B. in **Zeugniskonferenzen** Teilnahme- und Beratungsrechte der Elternvertreter bestehen. Häufig handelt es sich um Fälle, in denen Familien aufgrund nachbarrechtlicher oder anderer Streitigkeiten verfeindet sind. Im vergangenen Jahr fragte wiederum eine Schule an, ob Eltern der Information der Elternvertreter über Zeugnisnoten widersprechen können.

Das Bildungsministerium wies bislang immer darauf hin, daß die Klassenelternbeiratsvorsitzenden gesetzliche Mitglieder der Klassenkonferenz seien, bei Zeugnis- oder Versetzungskonferenzen zur Teilnahme mit beratender Stimme eingeladen würden und vor dem Hintergrund dieser im Gesetz festgelegten Position den Eltern der betroffenen Schüler kein Widerspruchsrecht gegen Informationen der Elternvertreter eingeräumt werden könne. Es gälten die allgemeinen Regeln des Verwaltungsverfahrensrechts, die entsprechende Einschränkungen nicht vorsähen. Überdies unterlägen die ehrenamtlich tätigen Elternvertreter der **Verschwiegenheitspflicht**. Wolle man hier in speziellen Situationen Sonderregelungen einführen, so dürfe das nur im Rahmen einer Gesamtschau über vergleichbare Verfahren geschehen, wie sie auch bei anderen Ausschuß-, Konferenz- und Gremienentscheidungen ablaufen.



Wir meinen, daß man ohne große Probleme in begründeten Konfliktfällen durch die Einräumung einer **Widerspruchsmöglichkeit** Abhilfe schaffen könnte. Die den Elternvertretungen mit ihrer Wahl übertragene Aufgabe, Rechte von Schülern und Eltern zu vertreten, läßt eine Parallele zu solchen ehrenamtlich tätigen Personen nicht zu, die die Allgemeinheit bzw. das Allgemeinwohl zu vertreten haben. Die Diskussionen mit dem Bildungsministerium über die Notwendigkeit, klarere Regelungen im Schulgesetz zu schaffen, werden fortgesetzt werden müssen.

Was ist zu tun?
Eltern sollte ein (zu begründendes) Widerspruchsrecht gegen die Unterrichtung des Elternbeirats über Angelegenheiten ihres Kindes eingeräumt werden.

übertrug den Namen und die Anschrift der Bank und die Kontonummer in den offenbar schon bereitgelegten Vordruck einer **„Pfändungs- und Einziehungsverfügung"**. Die Angaben über den Gläubiger entsprachen also den Daten der Anfrage, nicht aber denen der Rückmeldung des Energieversorgungsunternehmens.

Deshalb war die Personalstelle der Bank nicht wenig erstaunt, als von dem Konto ihres Direktors ein Betrag von 220 DM gepfändet wurde. Er selbst fiel aus allen Wolken, als er von seinen Mitarbeitern gefragt wurde, ob er sich mit dem Finanzamt nicht auf andere Weise einigen wolle.

Was war passiert? Unter der angegebenen Adresse fand das **Energieversorgungsunternehmen** keinen Kunden mit dem vom Finanzamt angegebenen Namen. Aber ein paar Häuser weiter hatte man besagten Namen registriert. Die Person war „offensichtlich" umgezogen, freundlicherweise teilte man dem Finanzamt gleich die neue Adresse mit. Das Finanzamt nahm diese aber gar nicht zur Kenntnis, es interessierte sich doch nur für das Konto und das dort vielleicht versteckte Guthaben. Auf diese Weise mußte der Herr Bankdirektor – sehr zu seinem Ärger – eine Gehaltspfändung erdulden, während sein Namensvetter sich darüber freute, daß das Finanzamt ihn ungeschoren ließ.

Was ist zu tun?
Immer wieder sind die Mitarbeiter von Behörden zu ermahnen, die Identität der Betroffenen sorgfältig zu überprüfen und Adreßdaten mit derselben Sorgfalt zu behandeln wie die vermeintlich viel wichtigeren „Falldaten".

4.10.3. Unmut über die Nutzung von Grundsteuerdaten für andere Zwecke

Die Lockerung des Steuergeheimnisses durch neue gesetzliche Ausnahmeregelungen läßt die Bürger immer häufiger fragen: „Was ist das Steuergeheimnis eigentlich noch wert?"

In der Praxis der Kommunen ist es „seit ewigen Zeiten" so üblich: Die Daten, die man auf den Grundsteuermeßbescheiden von den Finanzämtern erhält, werden nicht nur zur Erstellung der Grundsteuerbescheide verwandt. Sie dienen oft auch als Grundlage für die Festsetzung der Straßenreinigungs-, Müllabfuhr-, Abwasser- und sonstiger Gebühren. Viele Gemeinden führen ein regelrechtes **Grundeigentümerverzeichnis** und erteilen daraus Auskünfte.

Als die Datenschutzbeauftragten diese Vorgehensweise unter Hinweis auf das Steuergeheimnis beanstandeten, war guter Rat teuer. Zweifelsfrei ließ die Abgabenordnung eine solche Nutzung nicht zu; verzichten mochte man auf diese „Umwidmung" von Steuerdaten aber auch nicht. Die kommunalen Spitzenverbände konnten im Jahr 1993 erreichen, daß der Bundestag das **Steuergeheimnis** durch eine Änderung der Abgabenordnung **lockerte**. Es wurde festgelegt, daß besagte Namen und Anschriften von Grundstückseigentümern auch für die Verwaltung anderer Abgaben und zur Erfüllung sonstiger öffentlicher Aufgaben

mit den Worten umschrieben worden war: „Über Maßnahmen des Datenschutzes und der Datensicherung beim Einsatz automatischer Einrichtungen der DZ Schleswig-Holstein für Aufgaben der Steuerverwaltung entscheidet die OFD in eigener Verantwortung."

Mehr Klarheit schaffte eine erst im letzten Moment erlassene interne Dienstanweisung der OFD, wonach der Einsatz von Mitarbeiterinnen und Mitarbeitern der DZ Schleswig-Holstein zur Erledigung von Steuerverwaltungsaufgaben grundsätzlich unzulässig ist, weil es dadurch zu einer unbefugten **Offenbarung von Steuerdaten** kommen könnte. Dies gelte auch für die Erledigung unselbständiger technischer Hilfstätigkeiten in den Bereichen Druck, Kuvertierung und Versandvorbereitung. „Sollte ein solcher Einsatz aufgrund personeller Engpässe bei den Mitarbeitern der Steuerverwaltung zwingend erforderlich werden, entscheidet hierüber im Einzelfall der Gruppenleiter Automation der OFD." Aus unserer Sicht handelt es sich um eine Verfahrensweise, die dem Sinn des Steuergeheimnisses gerecht wird.

Was ist zu tun?
Nach einer angemessenen Frist, in der die Übergangsschwierigkeiten bereinigt sein sollten, werden wir uns durch eine Prüfung vor Ort von der konsequenten Beachtung der gesetzlichen Vorgaben und den Forderungen des Finanzausschusses des Landtages überzeugen.

4.10.2 Kontopfändung beim Herrn Bankdirektor

Nur weil in seiner Nähe ein säumiger Steuerzahler mit gleichem Namen wohnte, wurde das Konto eines Bankdirektors gepfändet. Eine Unachtsamkeit kratzte an seinem guten Ruf.

Immer wieder wird den Datenschützern vorgehalten, sie würden viel zu strenge Maßstäbe anlegen. Daten, die in jedem Briefkopf stünden, wie Name, Anschrift, Telefonnummer und Bankkonto, gehörten eigentlich von den Regelungen der Datenschutzgesetze ausgenommen. Wie könnten diese Daten denn Schaden anrichten? Antworten auf diese Frage und Hinweise auf die Notwendigkeit, mit allen personenbezogenen Daten datenschutzgerecht umzugehen, gibt es viele (vgl. z. B. 18. TB, Tz. 4.7.2). Auch im abgelaufenen Jahr wurde uns wiederum ein „klassischer Fall" aus dieser Kategorie bekannt.

Ein Finanzamt erfragte bei einem Energieversorgungsunternehmen die Bankverbindung eines Steuerschuldners, um eine **Kontopfändung** auszubringen. Alle dem Finanzamt bekannten Konten waren bereits erfolglos „abgegrast", es war dort kein Geld zu holen gewesen. Das Finanzamt bezeichnete den säumigen Zahler durch Name, Vorname, Straße, Hausnummer und Wohnort. Die befragte Stelle gab dem Finanzamt daraufhin die Bankverbindung einer Person mit gleichem Namen, gleichem Vornamen, einer abweichenden Straßenbezeichnung und einer abweichenden Postleitzahl/Ortsbezeichnung bekannt. Das Finanzamt wiederum

der Umfang des **Datenaustausches zwischen** den **Finanzämtern** und den **Kammern**. Schon als die Abgabenordnung noch „Reichsabgabenordnung" hieß, wurde festgelegt, daß die Finanzämter den Kammern jährlich die Besteuerungsgrundlagen mitzuteilen haben, die erforderlich sind, um die Kammerbeiträge festzusetzen. Dies ist ein Ausfluß der (zwischenzeitlich heftig kritisierten) Zwangsmitgliedschaft in den Kammern. Vielen Beitragspflichtigen war dieser Datenkanal bisher nur noch nicht aufgefallen.

Begeistert waren die Anrufer und Briefeschreiber natürlich nicht, als sie vom Datenschutzbeauftragten zu hören und zu lesen bekamen: Es besteht keine Möglichkeit zu datenschutzrechtlichen Beanstandungen; da kann nur der Gesetzgeber etwas ändern.

Was ist zu tun?
Die Kammern sollten sich Gedanken über eine etwas offensivere Aufklärung ihrer Mitglieder machen. Je transparenter die Datenströme für die Betroffenen sind, um so geringer ist das Risiko des Entstehens von Mißverständnissen, die nur mühsam wieder ausgeräumt werden können.

4.11 Personalwesen

4.11.1 Wenn die Gehaltspfändung beim Fachvorgesetzten landet

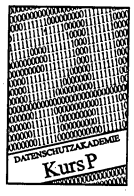
Der Fachvorgesetzte darf nur dann Kenntnis von Gehaltspfändungen gegen seine Mitarbeiter erhalten, wenn dies für dienstrechtliche Bewertungen und Entscheidungen notwendig ist.

Pfändungs- und Überweisungsbeschlüsse, die beim Landesbesoldungsamt eingehen, werden regelmäßig in Kopie an die jeweilige personalverwaltende Dienststelle übersandt, um dort die Prüfung zu ermöglichen, ob aufgrund der Pfändung weitere dienstrechtliche Maßnahmen notwendig sind. Bei einer **Polizeibehörde** war in einem konkreten Fall ein solcher Pfändungsbeschluß über einen Betrag von weniger als 300 DM auch dem **Fachvorgesetzten** des Betroffenen mit der Bitte um Stellungnahme vorgelegt worden und landete nach Anhörung des Betroffenen dann für drei Jahre in einem „besonderen Schrank". Hierbei handelte es sich nach unseren Feststellungen nicht um einen Einzelfall.

Um die Vertraulichkeit der Personalaktendaten zu sichern, wurde in das Dienstrecht eine Beschränkung des Personenkreises aufgenommen, der **Zugang zu Personalakten** erhalten darf. Danach haben Beschäftigte nur Zugangsberechtigung, die im Rahmen der Personalverwaltung mit der Verarbeitung von Personalangelegenheiten beauftragt sind, und nur, soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Im Unterschied zu anderen Verwaltungsvorgängen ist damit über den allgemeinen datenschutzrechtlichen Zweckbindungsgrundsatz hinaus eine besonders vertrauliche Behandlung von Personalvorgängen innerhalb der Verwaltung zu gewährleisten.

Geht es um einen Pfändungs- und Überweisungsbeschluß, muß der Betroffene dazu gehört werden. Danach ist eine dienstrechtliche Bewertung des Vorgangs notwendig, die zu dokumentieren ist. Ergeben sich aus der Bewertung dienstrechtliche Konsequenzen, sind die Unterlagen in die Personalakte aufzunehmen. Anderenfalls müssen die Unterlagen unverzüglich wieder aus der Personalakte entfernt und vernichtet werden.

In dem geprüften Fall war eine **Weiterleitung** des Pfändungs- und Überweisungsbeschlusses an den Fachvorgesetzten **nicht erforderlich**, da allein schon wegen der geringen Höhe des Betrages die abschließende dienstrechtliche Bewertung dem Leiter der Personalverwaltung möglich gewesen wäre. So mußten wir die Weiterleitung an den Fachvorgesetzten und die anschließende Aufbewahrung beanstanden.



Das **Innenministerium** machte Nägel mit Köpfen und nahm den Fall zum Anlaß, die Behandlung von Pfändungs- und Überweisungsbeschlüssen im Polizeibereich durch **Runderlaß** sachgerecht zu regeln.

Was ist zu tun?
Die Personalverwaltungen müssen dafür sorgen, daß die Federführung für die Bearbeitung von Pfändungs- und Überweisungsbeschlüssen bei ihnen liegt. Fachvorgesetzte dürfen nur informiert werden, soweit es im konkreten Einzelfall erforderlich ist. Ergeben sich nach einer Prüfung keine dienstrechtlichen Konsequenzen, ist der Vorgang unverzüglich zu vernichten.

4.11.2 Was der Amtsarzt dem Dienstherrn mitteilen darf

Geht ein Bediensteter zum Amtsarzt, ist zu unterscheiden, ob dies auf freiwilliger Basis oder auf gesetzlicher Grundlage geschieht. In dem einen Fall darf die Dienstbehörde nur mit Einwilligung, in dem anderen im Rahmen des Erforderlichkeitsprinzips unterrichtet werden.

Bei einer Lehrkraft war festgestellt worden, daß sie des öfteren alkoholisiert und unfähig war, den Schuldienst ordnungsgemäß wahrzunehmen. Der **Amtsarzt** wurde deshalb beauftragt, den Betroffenen auf mögliche Alkoholprobleme hin zu untersuchen. Der Betroffene erklärte sich mit einer Untersuchung einverstanden. Als er die Herausgabe der Untersuchungsergebnisse an den Dienstherrn verweigerte, wurden wir um Beratung gebeten. Für dienstrechtliche Entscheidungen bezüglich der gesundheitlichen Eignung von Beamten sieht das Landesbeamtengesetz die Einschaltung des Amtsarztes als Fachgutachter vor. Er

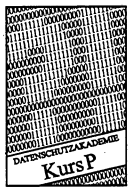
? Amtsarzt

Nach dem Gesundheitsdienst-Gesetz (GDG) haben die Kreise und kreisfreien Städte Gesundheitsämter zu unterhalten, deren Leiter die Aufgaben des Amtsarztes wahrnehmen. Sie haben in dieser Eigenschaft u. a. amtliche Gutachten und Zeugnisse auszustellen, soweit Rechtsvorschriften dies vorsehen (§ 22 GDG).

soll für den Dienstherrn ermitteln, ob und gegebenenfalls welche gesundheitlichen Einschränkungen des Betroffenen bei der Fortführung des bestehenden Dienstverhältnisses zu berücksichtigen sind.

Im vorliegenden Fall war aber lediglich der Auftrag erteilt worden zu prüfen, ob bei dem Betroffenen Anzeichen für einen Alkoholmißbrauch vorliegen und ihn gegebenenfalls über eventuelle erforderliche Therapiemaßnahmen zu beraten. Anhaltspunkte für eine generelle Dienstunfähigkeit waren (noch) nicht erkennbar. Eine Verpflichtung, sich untersuchen zu lassen, bestand für den Betroffenen nicht. Die Untersuchung erfolgte mithin auf **freiwilliger Grundlage**. Folglich war die Übermittlung des Untersuchungsergebnisses an den Dienstherrn ebenfalls nur auf freiwilliger Grundlage, d. h. mit Einwilligung des Betroffenen, zulässig.

Sofern der Dienstherr eine amtsärztliche Begutachtung aufgrund eines gesetzlichen Anspruchs veranlaßt, muß dies sowohl dem Betroffenen wie auch dem Amtsarzt gegenüber in dem **Gutachtenauftrag** zum Ausdruck gebracht werden. Nur unter dieser Voraussetzung hat der Betroffene dann die Möglichkeit zu prüfen, ob für ihn insoweit tatsächlich eine Obliegenheit zur amtsärztlichen Begutachtung besteht. Sind die gesetzlichen Voraussetzungen erfüllt, hat der Dienstherr dann einen Anspruch darauf, „die für die Feststellung der Dienstunfähigkeit erforderlichen Untersuchungsergebnisse durch die Ärztin oder den Arzt" mitgeteilt zu bekommen.



Dabei ist allerdings das **Erforderlichkeitsprinzip** zu beachten. Soweit Befunde keinen Anlaß für gesundheitliche Bedenken ergeben, sind sie für die Personalentscheidung nicht erforderlich und dürfen deshalb auch nicht übermittelt werden. Gibt es dagegen Gründe, die gegen eine Dienstfähigkeit sprechen, müssen sie, je nach Bedeutung, gegebenenfalls bis ins Detail dem Dienstherrn mitgeteilt werden, um ihm eine ordnungsgemäße dienstrechtliche Bewertung des Vorgangs zu ermöglichen. Diese Daten sind auch deshalb für den Dienstherrn unverzichtbar, weil er sie in einem belastenden Bescheid gegenüber dem Betroffenen zur Begründung seiner Entscheidung darstellen muß.

Was ist zu tun?
Personalverwaltungen sollten darauf achten, daß Gutachtenaufträge für amtsärztliche Untersuchungen eindeutig abgefaßt werden. Sie müssen insbesondere die Befugnisgrundlage sowie den Zweck der Untersuchung zweifelsfrei erkennen lassen.

4.11.3 Neuorganisation beim polizeiärztlichen Dienst notwendig

Das neue Landesbeamtengesetz macht im polizeiärztlichen Dienst eine sorgfältige Unterscheidung zwischen den Aufgaben bei der Krankenbehandlung, der Gewährung von Heilfürsorge und der gutachterlichen Tätigkeit notwendig. Die Aktenführung muß dementsprechend neu organisiert werden.

Polizeibeamte unterliegen wegen der von ihnen wahrzunehmenden Aufgaben in der Regel einem besonderen gesundheitlichen Risiko. Um die Bereitschaft zu einem notwendigen körperlichen Einsatz zu fördern, wurde für diese Personengruppe ein Anspruch auf **besondere Heilfürsorge** gegenüber dem Dienstherrn geschaffen. Es wurde ein eigener polizeiärztlicher Dienst eingerichtet, der die speziellen Anforderungen des Polizeivollzugsdienstes einschätzen kann und deshalb für die Behandlung wie auch für die Begutachtung von Erkrankungen der Polizeibeamten besonders qualifiziert ist.

Die im polizeiärztlichen Dienst tätigen Ärzte werden in **drei unterschiedlichen Funktionen** tätig:

- als behandelnder Arzt des Polizeibeamten,
- als Vertreter des Dienstherrn im Rahmen der Gewährung der Heilfürsorge,
- als Gutachter des Dienstherrn bei allgemeinen personalrechtlichen Entscheidungen, für die Fragen der gesundheitlichen Eignung von Bedeutung sind.

Prinzipiell steht es Polizeibeamten frei zu entscheiden, ob sie sich zur ärztlichen Behandlung an den Polizeiarzt wenden oder einen privaten Arzt ihrer Wahl aufsuchen. Neu eingestellte Beamte werden dagegen in der Regel innerhalb der ersten fünf Jahre ihrer Dienstzeit bzw. bis zur Erreichung des 25. Lebensjahres verpflichtet, den Polizeiarzt für Behandlungszwecke in Anspruch zu nehmen, wenn sie Leistungen aus der Heilfürsorge erhalten wollen. Der polizeiärztliche Dienst in der Polizeidirektion für Aus- und Fortbildung, der dort die Behandlungsaufgaben wahrnimmt, begutachtet üblicherweise auch die Polizeifähigkeit der Beamten nach Ablauf der Probezeit.

Soweit bisher im polizeiärztlichen Dienst schriftliche Unterlagen entstanden, wurden diese in einer **einheitlichen Krankenakte** zusammengefaßt. Die Aufsicht für den polizeiärztlichen Dienst oblag dem leitenden Polizeiarzt. Neben der ärztlichen Tätigkeit war er auch für die verwaltungsrechtlichen Entscheidungen über die Gewährung von Heilfürsorge sowie für die Erstellung von Gutachten für den Dienstherrn zuständig.

Das **neue Personalaktenrecht** hat nun auch im Bereich der Heilfürsorge eine räumliche, organisatorische und personelle Abschottung ausdrücklich vorgeschrieben, weil der Gesetzgeber hier die Möglichkeit unvertretbarer Interessenkollisionen gesehen hat. Die Gefahr der bewußten oder unbewußten Beeinflussung von Personalentscheidungen durch die Kenntnis von Heilfürsorgedaten oder

der Krankengeschichte (als behandelnder Arzt) ist ungleich höher als bei anderen Verwaltungsverfahren. Die Polizeidienststellen müssen deshalb die notwendigen räumlichen, organisatorischen und personellen Voraussetzungen für die Gewährleistung der vorgeschriebenen Abschottung der Heilfürsorge von der übrigen Personalverwaltung schaffen. Es sind dabei folgende Maßgaben zu berücksichtigen:

- Soweit Polizeiärzte als **behandelnde Ärzte** tätig werden, unterliegen die ihnen bekanntgewordenen Daten der ärztlichen Schweigepflicht, auch gegenüber dem Dienstherrn. Außer für die Abrechnung ist ihre Verwendung für andere Zwecke nur mit Einwilligung des jeweiligen Mitarbeiters zulässig. Die Dokumentationspflicht als behandelnder Arzt nach der ärztlichen Berufsordnung geht üblicherweise erheblich über die im Rahmen der Heilfürsorge erforderlichen Personalaktendaten hinaus. Es handelt sich auch begrifflich nicht um Personalaktendaten, so daß nicht die beamtenrechtlichen, sondern nur die für die ärztliche Dokumentation geltenden Verarbeitungsregelungen einschlägig sind. Gesundheitsdaten, die einem Polizeiarzt als behandelndem Arzt bekanntgeworden sind, dürfen also ohne Einwilligung der Betroffenen weder für Heilfürsorgezwecke noch für sonstige Gutachtertätigkeiten verwendet werden.
- Im Rahmen der **Heilfürsorge** werden dem polizeiärztlichen Dienst nicht nur Abrechnungsdaten, sondern darüber hinaus auch medizinische Daten bekannt (z. B. bei der Entscheidung über die Notwendigkeit einer Kur, einer psychotherapeutischen Behandlung o. ä.). Sämtliche Heilfürsorgedaten sind nach den Vorschriften des Landesbeamtengesetzes wie Beihilfedaten von der übrigen Personalverwaltung abzuschotten.
- Für allgemeine **beamtenrechtliche Entscheidungen** dürfen Daten aus der Tätigkeit des Polizeiarztes als behandelnden Arzt oder aus seiner Tätigkeit im Rahmen der Heilfürsorge nur mit ausdrücklicher Einwilligung des Betroffenen weiterverarbeitet werden. In Anbetracht des bestehenden Abhängigkeitsverhältnisses des Beamten von seinem Dienstherrn muß sorgfältig darauf geachtet werden, daß im Falle der Einwilligung auch tatsächlich eine freie Willensentscheidung für den Betroffenen möglich ist. Dies bedeutet, daß für ihn zumindest eine Alternative, bei der die gesetzlichen Zweckbindungsregelungen beachtet werden, vorhanden sein muß. In Betracht kommt die Einschaltung eines anderen Polizeiarztes oder des Amtsarztes.



Die Praxis im polizeiärztlichen Dienst entsprach bis zum Redaktionsschluß noch nicht den gesetzlichen Maßgaben. Die Krankenakten enthielten Unterlagen aus allen Tätigkeitsbereichen des ärztlichen Dienstes. Die Organisationsform des polizeiärztlichen Dienstes berücksichtigte noch nicht die erforderliche personelle Trennung der drei angesprochenen Tätigkeitsfelder. Ein besonderes Problem ist auch die Funktion des **leitenden Polizeiarztes**, der auf sämtliche Feststellungen und Entscheidungen des polizeiärztlichen Dienstes nicht zuletzt aufgrund seiner Aufsichtsfunktion erheblich einwirken kann. Da die Neuorganisation der Aktenführung jedenfalls auch von der künftigen Organisation des polizeiärztlichen Dienstes abhängig ist, sollte über letztere vorrangig entschieden werden.

Was ist zu tun?
Der polizeiärztliche Dienst muß unter Beachtung des Abschottungsgebotes für die Heilfürsorge reorganisiert werden. Außerdem müssen die vorhandenen einheitlichen „Krankenakten" gemäß den unterschiedlichen Zweckbestimmungen getrennt werden.

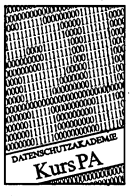
4.11.4 Akteneinsichtsrecht des Personalrats

Arbeitsvertragsentwürfe sind nicht Bestandteile der Personalakte. Sie müssen aber mit ähnlicher Sorgfalt behandelt werden.

Das schleswig-holsteinische Mitbestimmungsgesetz gewährt den Personalräten ein umfassendes Recht, bei Entscheidungen der Verwaltung in Personalangelegenheiten mitzubestimmen. Allerdings ist die **Einsichtnahme** in **Personalakten** nur bei ausdrücklicher Zustimmung der betroffenen Mitarbeiterinnen und Mitarbeiter und nur den von ihnen benannten Mitgliedern des Personalrats gestattet.

Eine Dienststelle fragte bei uns an, ob sie vor diesem Hintergrund verpflichtet sei, dem Wunsch des **Personalrates** zu entsprechen und ihm schon den Entwurf eines noch zu vereinbarenden Arbeitsvertrages zugänglich zu machen, der ein bestehendes befristetes Arbeitsverhältnis mit einem Mitarbeiter verlängern sollte. Der Personalrat gebe sich nicht mit einer Information über die zu vereinbarenden Vertragsdaten zufrieden, sondern bestehe darauf, den gesamten Entwurfstext vorgelegt zu bekommen.

Der bloße Entwurf eines Arbeitsvertrages entfaltet noch keine Rechtswirkung gegenüber dem Mitarbeiter und berührt damit nicht sein Grundverhältnis zur Beschäftigungsdienststelle. Er gehört formal noch nicht zur Personalakte. Auch die sichere Erwartung, er werde in absehbarer Zeit Personalaktenbestandteil, führt nicht zu einer Art „vorgezogener Personalakteneigenschaft". Allerdings ist die besondere, aus dem Personalaktenrecht herzuleitende **Schutzbedürftigkeit der Daten** zu berücksichtigen. Es kann daher in einem solchen Fall nicht ohne weiteres von einem Einsichtsrecht des Personalrats in Arbeitsvertragsentwürfe ausgegangen werden.



Enthält ein Entwurf nämlich mehr Daten, als der Personalrat für seine Entscheidungsfindung benötigt, muß von einer Einsichtnahme abgesehen werden. Statt dessen sind nur die tatsächlich erforderlichen Daten weiterzugeben. Was als erforderlich anzusehen ist, hängt von den Umständen des Einzelfalles ab.

Was ist zu tun?
Im Rahmen der Personalratsbeteiligung ist sorgfältig zu prüfen, von welchem Zeitpunkt an Informationen zu den Personalakten zu rechnen sind. Auch davor ist die Unterrichtung des Personalrates im Rahmen der Mitbestimmung auf die nach den Umständen des Einzelfalles dafür erforderlichen Daten zu beschränken.

4.12 Angekündigte unangekündigte Kontrollen

Bei Kontrollen des sorgsamen Umgangs mit personenbezogenen Daten zeigte sich ein differenziertes Bild: Neben eklatanten Schwächen war einiges auch weitgehend in Ordnung.

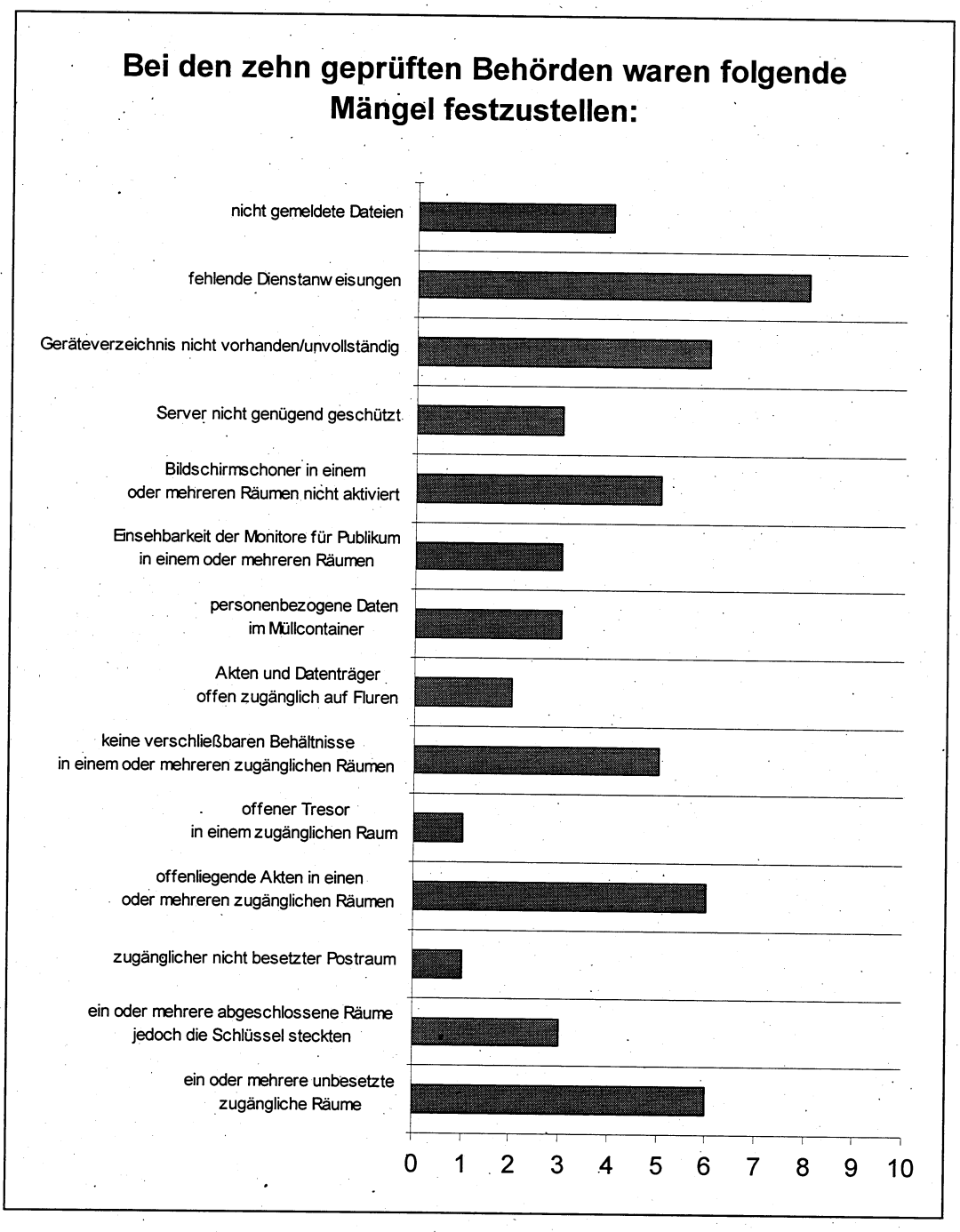
Im 19. Tätigkeitsbericht hatten wir bereits unser Konzept der angekündigten unangekündigten Kontrollen (AUK) vorgestellt (vgl. 19. TB, Tz. 1.1). Nachdem die Aktion im Jahre 1996 angelaufen war, konnten wir 1997 **zehn Prüfungen** durchführen. Zuvor hatten wir 50 Behörden angeschrieben und unsere unangekündigten Besuche in Aussicht gestellt. Aus diesen wurden dann die konkret geprüften Behörden ausgelost.

Die Ergebnisse zeigen, daß Kontrollen dieser Art durchaus sinnvoll sind. Gerade im Bereich des sorgsamen Umgangs mit personenbezogenen Daten gilt es, stets gegen Gleichgültigkeit und Sorglosigkeit anzugehen. Dies zeigt sich an folgenden Beispielen:

- Häufig haben wir Diensträume vorgefunden, deren **Türen** teilweise **sperrangelweit offenstanden**, ohne daß jemand im Raum war. Stets aber lagen in diesen Fällen Akten mit personenbezogenen Unterlagen frei zugänglich im Raum.
- In einem Fall haben wir uns über 10 Minuten lang im Büro des Leiters eines Sozialamtes aufgehalten, in dem größere Mengen von **Akten mit Sozialdaten** lagen, in die wir ungehindert Einsicht nehmen konnten. Auch hier stand die Bürotür zum Flur hin weit offen. Auf die vorgefundene Situation angesprochen, meinte der Beamte achselzuckend: „Eigentlich wollte ich nur für ganz kurze Zeit mein Büro verlassen."
- In einem Gericht fanden wir im **Papierkorb** neben dem Kopiergerät die Kopie einer richterlichen Entscheidung in einem Strafverfahren, inklusive Name des Betroffenen. Besonders brisant war die Angelegenheit, weil der Papierkorb auf dem offenen Flur stand.
- Mehrfach haben wir auch festgestellt, daß personenbezogene Daten in Altakten, also Vorgängen, die bereits auf ihre Vernichtung warten, offensichtlich nicht mehr als schützenswert angesehen werden. Wir fanden in einigen Fällen offene Kellerräume, in denen Vorgänge mit personenbezogenen Daten gelagert waren. Auch kam es vor, daß zur Vernichtung bestimmte Unterlagen in **offenen Müllsäcken** in frei zugänglichen Kellerfluren auf ihre Abholung warteten.
- Die EDV-technische Ausstattung der einzelnen Verwaltungen wurden von uns nur stichprobenartig auf ihre Sicherheit überprüft. Auch hier mußten wir feststellen, daß teilweise nicht sorgfältig vorgegangen wurde, manchmal fehlten die einfachsten Sicherheitsvorkehrungen. Häufig stellten wir fest, daß die Mitarbeiter, die mit ihren Datenverarbeitungsanlagen tagtäglich arbeiten müssen, nicht ausreichend über die datenschutzrechtlichen Aspekte beim Umgang mit den elektronischen Medien geschult worden sind, obwohl das

Landesdatenschutzgesetz diese Schulung ausdrücklich verlangt.

Die nachfolgende Tabelle vermittelt einen Überblick über die bei den zehn Behörden gefundenen Schwachpunkte:



Die Ergebnisse unserer Kontrollen wurden mit den Verwaltungen besprochen. In Fällen, in denen von uns Beanstandungen ausgesprochen wurden, wurden kurzfristig Verbesserungen vorgenommen. Interessant ist noch folgendes: In vielen Fällen waren die Mitarbeiter der geprüften Verwaltungen froh über unser Erscheinen. Denn sie hatten oftmals bereits an die Verwaltungsleitung Mängel gemeldet, ohne daß Abhilfe geschaffen wurde. Sie sahen sich durch uns bestätigt.

5. Datenschutz bei den Gerichten

5.1 Videoüberwachung im Sozialgericht

Die Videoübertragung in der Antragsstelle eines Sozialgerichts verletzte das Sozialgeheimnis. Sie wurde inzwischen eingestellt.

In der Rechtsantragsstelle eines Sozialgerichtes wurde aus Sicherheitsgründen zum Schutzes der dort allein tätigen Mitarbeiterin eine Videoanlage installiert, durch die eine Bild- und Tonübertragung des Publikumsverkehrs in die Pförtnerloge vorgenommen wurde. Sobald eine Person in den Raum eintrat, um einen Antrag oder eine Klage in sozialrechtlichen Angelegenheiten anzubringen, schaltete die Mitarbeiterin die Anlage ein, so daß in der Pförtnerloge nicht nur der Antragsteller beobachtet, sondern auch sämtliche Inhalte der von ihm vorgebrachten Angelegenheit mitgehört werden konnten. Die Antragsteller wurden vorab auf die Existenz der **Überwachungsanlage** hingewiesen, worauf es in mindestens einem Fall dazu kam, daß der Betroffene eine Antragstellung verweigerte. Der Sachverhalt wurde uns bekannt, nachdem mehrere Personen, die offenbar das interessante „Fernsehprogramm" beim Pförtner mitverfolgen konnten, sich empört an uns wandten.

Der Direktor des Sozialgerichtes verwies in seiner Stellungnahme darauf, daß die Anlage ausschließlich (allerdings nicht näher konkretisierten) Sicherheitsinteressen der Mitarbeiterin diene und hierfür ein einfacher Alarmknopf nicht ausreiche, weil er von der Mitarbeiterin nicht in allen Situationen erreicht werden könne.

Daß die dem **Sozialgeheimnis** unterliegenden, besonders schützenswerten Informationen, die ein Antragsteller beim Sozialgericht offenbart, anderen sachlich nicht zuständigen Bediensteten des Gerichts sowie darüber hinaus unbeteiligten Passanten zur Kenntnis gelangen konnten, war ein schwerer Verstoß gegen Datenschutzrecht. Das Landesdatenschutzgesetz erlaubt zur Wahrung von Sicherheitsbelangen im Rahmen des Hausrechts von vornherein allenfalls eine Bild- und keine Tonübertragung bei der Überwachung öffentlich zugänglicher Räume. Auch eine Bildübertragung darf nur stattfinden, wenn nicht schutzwürdige Belange Betroffener überwiegen. Im vorliegenden Fall war auch eine Bildübertragung unzulässig, da sie von Dritten eingesehen werden konnte und nach der Argumentation des Sozialgerichtsdirektors nicht nachvollziehbar war, warum auf der Rechtsantragsstelle über die sonst in vergleichbaren Bereichen üblichen Alarmsysteme hinausgegangen werden mußte.

Die Video- und Tonübertragungsanlage wurde inzwischen abgeschafft.

Was ist zu tun?
Bei der Lösung von Sicherheitsproblemen in öffentlichen Stellen sollte nicht sofort zur technischen „Maximallösung" gegriffen werden, bevor die Auswirkungen auf die Persönlichkeitsrechte von Betroffenen bedacht sind.

5.2 Gerichtsaushänge in Verfahren auf Abgabe der eidesstattlichen Versicherung

Die Eintragung des Namens in die Terminsrolle bei den Gerichten führt zu einer unnötigen Bekanntgabe der Personen, die zur Abgabe der eidesstattlichen Versicherung geladen sind.

In den Gerichten befinden sich an den Eingängen zu den Verhandlungsräumen sogenannte Terminsrollen, aus denen die Namen der beteiligten Parteien zu ersehen sind. Dies ist unproblematisch, soweit das gerichtliche Verfahren ohnehin öffentlich ist. Eine andere Situation liegt jedoch vor, wenn, wie bei den Verfahren auf Abgabe der **eidesstattlichen Versicherung,** keine öffentliche Verhandlung stattfindet. Denn durch den Aushang können Dritte erfahren, welche Personen zur Abgabe einer solchen Erklärung verpflichtet werden sollen, ohne daß sie ein Recht auf Teilnahme an dem Verfahren hätten noch sonstwie eine Notwendigkeit zu ihrer Unterrichtung bestünde. Gelegentlich kommt es außerdem gar nicht zur eidesstattlichen Versicherung, weil der Schuldner im Termin bezahlt.

Wir haben deshalb dem Justizministerium des Landes Schleswig-Holstein empfohlen, das Verfahren zu ändern. Es sollte allenfalls das Aktenzeichen in die Terminsrollen eingetragen werden. Die Raumnummer sowie das Aktenzeichen kann der Betroffene der Ladung entnehmen, die er von dem Gericht erhalten hat. Um dies umzusetzen, hält das Ministerium eine Änderung der **bundeseinheitlichen Aktenordnung** für erforderlich und hat deshalb die Justizverwaltungen der Bundesländer sowie das Bundesministerium der Justiz zur Stellungnahme aufgefordert. Da es sich nicht um ein Gesetz, sondern bloß um eine interne Verwaltungsvorschrift handelt, könnte das Verfahren nach unserer Auffassung auch ohne bundeseinheitlichen „Segen" jetzt schon datenschutzgerechter gestaltet werden. So hat auch der Justizminister von Mecklenburg-Vorpommern veranlaßt, daß dort künftig in allen nichtöffentlichen Verfahren der Name des Betroffenen auf der Terminsrolle entfällt.

Mittlerweile hat der Gesetzgeber die Zuständigkeit für die Abnahme der eidesstattlichen Versicherung ab dem 01.01.1999 auf die Gerichtsvollzieher verlagert. Im Hinblick hierauf möchte der **Justizminister** von einer Änderung der Aktenordnung absehen und bis dahin lediglich den Hinweis auf die Verfahrensart auf Terminsrollen streichen. Damit wäre jedoch die Chance einer datenschutzgerechten Interimslösung verpaßt; die geschilderte Problematik bliebe zudem für alle anderen nichtöffentlichen Verfahren bestehen.

Was ist zu tun?
Die Aktenordnung sollte in der Weise modifiziert werden, daß bei nichtöffentlichen Verhandlungen nicht mehr die Namen der Beteiligten, sondern nur noch die Aktenzeichen in die Terminsrolle eingetragen werden.

6. Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung

6.1 30 Jahre EDV in der Verwaltung – und kein bißchen weise?

Seit langem bekannte gravierende sicherheitstechnische Problemstellungen sind von den Behörden auch im Verlaufe der letzten 10 Jahre nicht gelöst worden. Der Drang nach immer mehr Informationstechnik vergrößert die Risiken.

In einem Schreiben mit Datum vom 21.10.1968 teilte der damalige Ministerpräsident seinen Kabinettskollegen mit, daß die Datenzentrale Schleswig-Holstein nunmehr ihre Arbeit in vollem Umgang aufgenommen habe, um die Erledigung von Aufgaben der öffentlichen Verwaltung im Lande durch Computer zu ermöglichen. Die damaligen EDV-Entscheidungsträger dürften zwischenzeitlich aus dem aktiven Dienst ausgeschieden sein und ihre Erfahrungen an die nächste Generation der Datenverarbeiter weitergegeben haben, in vielen Verwaltungen haben bereits die „Enkel" die Verantwortung übernommen. Vor dem Hintergrund, daß das Datenschutzrecht zwanzig dieser dreißig Jahre „regelnd und steuernd" begleitet hat, sollte man annehmen, daß alle wesentlichen und grundsätzlichen sicherheitstechnischen Problemstellungen, die beim Einsatz von Computern zur Bewältigung der personenbezogenen Datenverarbeitung in der Verwaltung auftreten und einer allseits befriedigenden Lösung zugeführt worden sind. **Dreißig Jahre Erfahrung** mit den technischen Systemen und zwanzig Jahre Erfahrung mit den Datensicherheitsvorschriften sollten ausreichen, um Kinderkrankheiten zu überwinden und um im Tagesgeschäft der Praxis Datensicherheit und Ordnungsmäßigkeit der Datenverarbeitung auf einem hohen Niveau zu gewährleisten, auch wenn ständig technische Neuerungen einzubinden sind.

Das Ende einer Dekade gibt Anlaß zu einer vergleichenden Betrachtung und einem Resümee. So ist es vor zehn Jahren geschehen (vgl. 10. TB, Tz. 1) und das **Fazit** lautete **1987**: Das Datenschutzrecht hat in zehn Jahren mehr bewirkt als zunächst zu erwarten war. Es sind aber nicht alle Probleme gelöst worden, die bei konsequenter Umsetzung der gesetzlichen Bestimmungen lösbar gewesen wären.

Weitere zehn Jahre später stellt sich erneut die Frage nach Defiziten inhaltlicher und methodischer Art. Deshalb soll die nachfolgende Darstellung der kritischen Anmerkungen aus den Tätigkeitsberichten der Jahre 1986 bis 1988 den Vergleich mit der heutigen Situation ermöglichen. Einige der damaligen Schlagzeilen lauteten:

- Vorgesetzte stehlen sich aus der Verantwortung für die technischen Systeme *(9. TB, Tz. 5.3)*
- Es mangelt an der Beherrschbarkeit und Revisionsfähigkeit der EDV-Systeme *(9. TB, Tz. 5.3)*
- Mangelhafte Tests und unklare Verantwortlichkeiten bei Verfahrensfreigaben *(10. TB, Tz. 7.2)*

- Ungelöste Rechtsprobleme bei der Abrechnung von Krankenhausleistungen in externen Rechenzentren
  (9. TB, Tz. 4.5.3)
- Technische Systeme schaffen vollendete Tatsachen, die Datensicherheit wird erst später und dann meist unzulänglich aufgepfropft
  (9. TB, Tz. 5.3)
- Der Funkverkehr der Polizei und der Rettungsdienste ist nicht abhörsicher
  (9. TB, Tz. 4.1.5.3)
- Krankenhausinformationssysteme versus ärztliche Schweigepflicht
  (10. TB, Tz. 5.2)
- Probleme bei der Nutzung privater PC für dienstliche Zwecke
  (11. TB, Tz. 5.6)
- Sicherheitsmängel bei (unausgereiften) Pilotprojekten
  (11. TB, Tz. 7.1)
- Computer-Viren und unkontrollierter PC-Einsatz gefährden die Datensicherheit
  (11. TB, Tz. 7.2)

Betrachtet man das Inhaltsverzeichnis des vorliegenden Tätigkeitsberichtes und das der Tätigkeitsberichte der letzten Jahre, wird man feststellen, daß die Verantwortlichen kaum eines der vorstehenden – immerhin zehn Jahre alten – Probleme zwischenzeitlich in den Griff bekommen haben. Dies muß als ein **Alarmsignal** betrachtet werden. Zu den bekannten Defiziten kommen nämlich offensichtlich immer neue hinzu. Zu nennen sind in diesem Zusammenhang:

- Nutzung unsicherer Netze,
- Einschaltung von immer mehr externen Dienstleistern,
- fehlende technische Ausbildung von Systembetreuern,
- Undurchschaubarkeit technischer Lösungen,
- Allmacht der Anbieter von Standard-Software,
- Infiltration von IT-Systemen durch unbefugte externe Benutzer,
- Kontrolldefizite bei grenzüberschreitendem Datenverkehr und
- Dokumentations- und Protokollierungsmängel bei komplexen IT-Systemen.

Wer nur den Ausstattungsgrad der Behörden mit PC an den Arbeitsplätzen als Maßstab sieht, der wird stolz auf die zurückliegenden zehn Jahre blicken können. Wer sich aber die Kriterien „**Beherrschbarkeit**“, „**Sicherheit**“ und „**Revisionsfähigkeit**“ der Informationstechnik auf die Fahnen geschrieben hat, der wird auch nach dreißig Jahren EDV-Entwicklung und nach zwanzig Jahren Datensicherheitsrecht mit dem gleichen, wenn nicht gar mit größeren Sorgen als vor zehn Jahren die Tagesaktualität und die künftigen Entwicklungen betrachten. Dies ist

aus der Sicht der von der Datenverarbeitung der öffentlichen Verwaltung betroffenen Bürger kein beruhigendes Fazit. Sie werden zu Recht die Frage nach der Verantwortung für diese Situation stellen.

Was ist zu tun?
Die Entscheidungsträger sollten einen neuen Kurs bei der Planung und Realisierung von Informationssystemen steuern: weg von der Masse – hin zur Klasse, aber auch: weg vom hektischen Aktionismus – hin zu soliden und dauerhaften Lösungen.

6.2 Automationskommission der kommunalen Landesverbände – gute Vorsätze drohen zu verwässern

Das Konzept für ein effektives Testverfahren für Kommunalsoftware ist seit einem Jahr fertig. Es schmort in der Schublade, weil man sich nicht über die Finanzierung einigen kann.

Das Thema „Test von Hard- und Softwareprodukten für den kommunalen Bereich" ist bereits in vielen Tätigkeitsberichten angesprochen worden (vgl. 13. TB, Tz. 6.3, 19. TB, Tz. 6.3). Es geht dabei seit Jahren um immer die gleiche Frage: Wie kann man erreichen, daß sich nicht jede kleine Amtsverwaltung erneut von der richtigen Funktionsweise der von der Datenzentrale oder anderen Anbietern erworbenen Programme oder Paketlösungen überzeugen muß? Allen Beteiligten ist klar, daß es viel effektiver wäre, wenn einige kompetente Kommunen diese Prüfungen vornehmen und hierüber Testate erstellen würden, auf die sich die anderen dann verlassen könnten.

Wie im letzten Tätigkeitsbericht dargestellt, hat die Automationskommission der kommunalen Landesverbände hierzu ein in sich **schlüssiges**, alle derzeitigen Defizite behebendes **Konzept** erarbeitet, an dem wir beratend mitgewirkt haben. Die Entscheidungsgremien der kommunalen Landesverbände haben dieses auch zustimmend zur Kenntnis genommen. In einem Punkt halten sie sich aber nun schon ein ganzes Jahr „bedeckt": Das Verfahren funktioniert nur dann, wenn eine zentrale Überwachung erfolgt. Die Anbieter von Hard- und Software brauchen eine Ansprechstelle; die ordnungsgemäße Durchführung der Tests muß kontrolliert werden, die Testate und Freigabeempfehlungen müssen dokumentiert werden, es muß überwacht werden, daß die Anbieter die Freigabeempfehlungen nicht unbefugt verwenden usw.

Dies alles ist der Automationskommission und den Kommunen seit langem klar, weil die erheblichen Arbeitsersparnisse bei den einzelnen datenverarbeitenden Stellen selbstverständlich an einer anderen Stelle einen (natürlich sehr viel geringeren) hohen Aufwand erzeugen. Kurz und gut: Die Automationskommission braucht einen **hauptamtlichen Geschäftsführer** und keiner will ihn bezahlen. Solange aber kein Geld zur Verfügung steht, bleibt auch das schöne Konzept in der Schublade liegen, und die Kommunen setzen weiterhin Software ein, die nicht

ausreichend getestet worden ist. Die Bürgermeister und leitenden Verwaltungsbeamten ärgern sich darüber. Sie schimpfen und fragen nach dem Sinn und Zweck der Automationskommission. Der Datenschutzbeauftragte legt bei allen Beratungsgesprächen und Überprüfungen sowie in seinen Tätigkeitsberichten erneut den Finger in die Wunde, aber ... nichts Entscheidendes passiert.

Vielleicht sind die Anbieter die einzigen, die sich (natürlich hinter verschlossenen Türen) die Hände reiben. Sie verkaufen ihre Produkte, auch **ohne** daß sie einer **strengen Kontrolle** unterzogen worden sind. Praktisch alle Verträge enthalten Klauseln wie: „Das Programm gilt als abgenommen, wenn binnen 30 Tagen keine Mängelreklamation erfolgt ist." Welcher Leiter eines Meldeamtes mit zwei bis drei Mitarbeitern kann z. B. ein komplexes Einwohnerinformationssystem (vgl. Tz. 9) innerhalb dieser kurzen Frist auf Herz und Nieren prüfen? Wer den Nutzen hat und wer den Schaden, braucht nicht näher erläutert zu werden.

Dabei geht es nicht nur um datenschutzrechtlich und sicherheitstechnisch relevante Verfahrensmängel. Wenn nicht schnell gehandelt wird, stehen die kleinen Kommunen auch bei der Umstellung auf den Euro und bei dem Jahrtausendwechsel programmtechnisch „allein und im Regen".

Was ist zu tun?
Das, was bereits vor einem Jahr hätte getan werden sollen. Deshalb ist unsere Forderung aus dem 19. Tätigkeitsbericht zu wiederholen: Zum eigenen Nutzen, insbesondere aber zum Nutzen der betroffenen Bürger, sollten die Empfehlungen der Automationskommission kurzfristig in die Tat umgesetzt werden.

6.3 PERMIS – wie die Technik den Weg diktiert

Während überall zentralisierte EDV-Verfahren abgelöst und die Datenbestände vor Ort vorgehalten werden, schwimmt man ausgerechnet bei der Personaldatenverwaltung gegen den Strom. Aus „Kostengründen" können diese sensiblen Daten nicht in den Personalstellen gespeichert, sondern „müssen" in ein zentrales Rechenzentrum übertragen werden.

Traditionell geht man in der Verwaltung mit den Personalakten eigentlich sehr sorgfältig um. Es mögen zwar häufig viel zu viele Daten erhoben und gespeichert werden, aber kaum ein Datenbestand wird so gut abgeschottet wie die Personalakten. Es fehlt nicht an verschließbaren Stahlschränken; Aktenböcke und Schreibtische werden bei Dienstschluß abgeräumt; selbst der Aktentransport innerhalb der Behörde erfolgt in der Regel in versiegelten Aktendeckeln. Da hätte es des neuerdings in § 106 a Landesbeamtengesetz (LBG) gesetzlich geregelten **besonderen Personaldatengeheimnisses** (vgl. 19. TB, Tz. 4.11.3) eigentlich gar nicht bedurft, wenn denn nicht auch in diesem Bereich zwischenzeitlich die Informationstechnik ihren Einzug gehalten hätte.

In den nächsten Monaten soll nämlich in allen Ressorts ein automatisiertes Verfahren zur Verwaltung von Personaldaten mit dem Namen **PERMIS** eingesetzt werden, das auch eine Schnittstelle zu einem Personalcontrollingsystem enthält, welches wiederum eine bessere Finanzkontrolle über die Personalkosten ermöglichen soll.

Man hätte eigentlich erwarten können, daß dieses Verfahren dem gleichen **Abschottungsprinzip** gehorcht wie die papierene Personaldatenverarbeitung. Folgendes Szenario wäre naheliegend gewesen: Im Zimmer des Personalreferenten steht ein Abteilungsrechner speziell für Personaldaten, dessen Administration durch Techniker nur in seinem Beisein möglich ist. Dieses Gerät ist nur mit den Arbeitsplatzrechnern der Personalsachbearbeiter vernetzt; alle Personaldaten sind zentral gespeichert; wer nicht Mitarbeiter der Personalstelle ist, bekommt keinen Kontakt mit den Datenbeständen.

? *PERMIS*

*Mit dem **P**ersonal-**M**anagement und **I**nformationssystem dürfen Daten der Mitarbeiter der betreffenden Behörden „nur für dienstliche Zwecke der Personalplanung und -betreuung sowie der Stellenbewirtschaftung verarbeitet werden, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung von Dienst- oder Arbeitsverhältnissen oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist.“*

Bei dem Verfahren PERMIS hat man sich allerdings für Programme entschieden, die eine sehr aufwendige Datenbanksoftware voraussetzen, obwohl die meisten Behörden nur wenige hundert Datensätze zu verwalten haben. Da diese Software außerdem noch hohe Lizenzgebühren kostet, lief das Verfahren Gefahr, für viele Behörden unwirtschaftlich zu werden. Dies wurde allerdings erst bemerkt, als die Programme bereits fertig waren. Um die Investitionen zu retten und um den kurzfristigen Einsatz des Personalmanagementsystems nicht zu gefährden, warf man das Abschottungsprinzip kurzerhand über Bord und wählte die Lösung **„PERMIS-Zentral“**. Zentral bedeutet nichts anderes, als daß jeder zu speichernde Personaldatensatz zunächst über das Campus-Netz (vgl. Tz. 6.7.6) in den Bereich des Innenministeriums und von dort im Rahmen des Schleswig-Holstein-Netzes (vgl. Tz. 6.7.7) in die Datenzentrale übertragen wird. In der DZ stehen wiederum Server, die die Personaldaten in separaten Datenbeständen speichern. Bei jeder Auswertung werden die betreffenden Datensätze auf dem gleichen Wege zurückübertragen. Das ganze rechnet sich nur deshalb, weil nicht jede Behörde einzeln, sondern die DZ nur einmal die Lizenzgebühren für die Datenbank-Software zu zahlen hat. Hätte man von vornherein eine billigere Datenbank-Konzeption gewählt, wäre wohl keine Personalstelle auf die Idee gekommen, z. B. für zweihundert Datensätze eine Datenbank im Großrechenzentrum in Altenholz anzulegen, anstatt sie auf dem zumeist ohnehin vorhandenen Rechner des Personalreferenten zu speichern.

Selbst wenn man unserer Forderung nach einer Verschlüsselung der Daten auf dem Transportweg folgt und die Aktivitäten der Systemadministrationen im Innenministerium und in der Datenzentrale sorgfältig überwacht, es bleibt nur die

zweitbeste Lösung. Jedenfalls ist es ein Musterbeispiel dafür, daß nicht die Logik, sondern vermeintlich technische Zwänge (oder „nur" eine Fehlentscheidung bei der Softwareauswahl?) das Ergebnis bestimmt haben.

Was ist zu tun?
Es sollte noch einmal geprüft werden, ob die Lösung „PERMIS-Zentral" wirklich der Weisheit letzter Schluß ist. Zumindest sollte bei künftigen Projekten nicht dieselbe „Methode" angewendet werden.

6.4 Datenschutzrechtliche Einordnung von Telearbeit

Im Zeichen des immer breiteren Einsatzspektrums der Informationstechnik wird die „Heimarbeit" wieder interessant. Unternehmen und Verwaltungen planen Telearbeitsplätze und sehen sich mit vielfältigen sicherheitstechnischen Problemen konfrontiert.

Immer mehr Behörden prüfen derzeit, ob mit der Einrichtung von Telearbeitsplätzen nicht zwei Fliegen mit einer Klappe zu schlagen sind. Zum einen könnten gut ausgebildete und erfahrene Mitarbeiter davon abgehalten werden, aus dem Berufsleben auszuscheiden, wenn sie z. B. aus familiären Gründen nicht mehr in der Lage sind, täglich ihren Arbeitsplatz in der Behörde aufzusuchen. Zum anderen bräuchte man für **Telearbeiter** keinen Büroraum vorzuhalten, was Kosteneinsparungen verspricht. Obwohl es typische „Heimarbeiter" bereits seit langem auch in der Verwaltung gibt (z. B. Gerichtsvollzieher, Lehrer, Betriebsprüfer), besteht bei den Behörden offenbar eine große Verunsicherung darüber, wie man speziell technikgestützte Arbeitsplätze so ausgestalten kann, daß neben dienstlichen Aspekten auch die datenschutzrechtlichen und sicherheitstechnischen Anforderungen erfüllt werden.

Auf Einladung der Technologie-Transfer-Zentrale haben wir uns deshalb an sogenannten Workshops beteiligt, in denen sich Unternehmensberater, Hard- und Softwareanbieter sowie interessierte Wirtschaftsunternehmen und Verwaltungen zusammenfinden und die vielfältigen betriebswirtschaftlichen, arbeitsrechtlichen, mitbestimmungsrechtlichen und eben auch sicherheitstechnischen Fragestellungen diskutieren. Wir haben in diesen Gesprächen geraten, für die Telearbeitsplätze die Vorschriften über die **Auftragsdatenverarbeitung** analog anzuwenden.

Es macht nämlich keinen gravierenden Unterschied, ob es sich bei dem „externen Dienstleister" um einen selbständigen Unternehmer oder um einen Mitarbeiter handelt. Entscheidend ist, daß in beiden Fällen die datenverarbeitende Stelle die unmittelbare Verfügungsgewalt über die Daten verliert. Die **Organisationshoheit** eines Dienststellenleiters endet nun einmal an der Haustür seiner Behörde. In den häuslichen Bereich seines Mitarbeiters kann er nur auf der Basis einer ausdrücklichen vertraglichen Vereinbarung hineinwirken. Andererseits muß kein Bürger dulden, daß sein Recht auf eine hinreichend abgesicherte Verarbeitung seiner personenbezogenen Daten deshalb eingeschränkt wird, weil aus Kostengründen

die Behörde nur noch „virtuell" besteht und die Daten tatsächlich „in den Wohnzimmern der Bediensteten herumschwirren".

Aus den gesetzlichen Regelungen zur Auftragsdatenverarbeitung lassen sich für Telearbeitsplätze zum Beispiel die folgenden grundsätzlichen **Sicherheitsanforderungen** ableiten:

- Die Pflichten der betreffenden Mitarbeiter sind schriftlich in Verträgen und Dienstanweisungen zu definieren.
- Die benutzten IT-Geräte sollten grundsätzlich im Eigentum der Verwaltung stehen und von ihr konfiguriert sein.
- Verändernde Zugriffe auf die Betriebssystemebene und auf Programme sollten nur der zentralen Systemadministration möglich sein.
- Sofern Datenbestände vor Ort vorgehalten werden müssen, sind sie zwangsweise zu verschlüsseln. Die Verschlüsselungsmethode und die Schlüssel sind von der Zentrale vorzugeben.
- Nicht mehr erforderliche Daten sind automatisch zu löschen.
- Die Benutzung der IT-Geräte ist nur demjenigen zu ermöglichen, der durch Paßworteingabe seine Legitimation nachweisen kann. Eingeschaltete Geräte sind automatisch zu sperren, wenn die Benutzer in einem bestimmten Zeitraum keine Aktivitäten entwickeln.

Im Wortlaut: § 4 LDSG (Auszug)

Läßt eine datenverarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Rechte der Betroffenen sind ihr gegenüber geltend zu machen.

Die datenverarbeitende Stelle hat dafür Sorge zu tragen, daß personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der ... notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen ...

Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.

Sofern die Vorschriften dieses Gesetzes auf Auftragnehmende keine Anwendung finden, hat die datenverarbeitende Stelle diese zu verpflichten, jederzeit von ihr veranlaßte Kontrollen zu ermöglichen ...

- Der Datenaustausch mit der Zentrale sollte nur in verschlüsselter Form erfolgen. Das gilt insbesondere für den Datenträgeraustausch per Disketten.
- Zur Verwahrung von Datenträgern, insbesondere papierener Unterlagen, sind verschließbare Behältnisse zur Verfügung zu stellen.
- Der Arbeitgeber muß für sich selbst und für den Landesbeauftragten für den Datenschutz ein Kontrollrecht in der Wohnung des Mitarbeiters ausbedingen.

- Entsprechende Kontrollen sollten für beide Seiten eine Selbstverständlichkeit sein.
- Gravierende Verstöße gegen die Vereinbarungen sollten eine fristlose Beendigung des Arbeitsverhältnisses zur Folge haben.

Bei allen Sicherheitsüberlegungen darf aber nicht übersehen werden, daß in bestimmten Bereichen eine Heimarbeit aus Rechtsgründen von vornherein ausscheidet bzw. von der Einwilligung der Betroffenen abhängig ist. Das gilt z. B. für die Verarbeitung medizinischer Daten, die der ärztlichen Schweigepflicht unterliegen (vgl. 18. TB, Tz. 4.8.3), für Verschlußsachen und für sonstige vertrauliche Datenbestände.

Was ist zu tun?
Bereits bei der Planung von Telearbeitsplätzen sind Sicherheitskonzepte zu erstellen, die die tatsächlichen, örtlichen und personellen Gegebenheiten berücksichtigen.

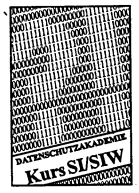
6.5 Wenn externe Berater das Konzept für das IT-System machen

Wer einen externen Berater einschaltet, um sich ein IT-Konzept entwickeln zu lassen, kann nicht immer auf zufriedenstellende Ergebnisse vertrauen. In vielen Fällen resultieren die Verfahrensmängel nicht aus der schlechten Arbeit der Berater, sondern aus fehlenden Vorgaben und Abstimmungen.

Wenn es um die Planung von neuen IT-Systemen geht, stehen viele Verwaltungen mangels hinreichenden Fachwissens „auf verlorenem Posten". Einige versuchen, sich mit dem Mut zum Risiko durchzulavieren, die Vorsichtigeren engagieren externe Berater, die für entsprechende Honorare sogenannte **IT-Konzepte** erstellen. Verständlicherweise geht man in diesen Fällen aber allzuhäufig davon aus, daß etwas, was viel Geld kostet, auch gut sein muß. Wenn dann die Planungs- in die Realisierungsphase und diese dann schließlich in den Echtbetrieb übergeht, stellt man nicht selten fest, daß viele der dann auftretenden Probleme nicht oder nur unzulänglich in dem IT-Konzept behandelt worden sind. Besonders überrascht ist man, wenn wir im Rahmen von Prüfungen (vgl. Tz. 6.7) Sicherheitslücken entdecken, deren Vermeidung der externe Berater gerade gewährleisten sollte.

Das Bestehen derartiger Defizite deutet allerdings nicht in jedem Fall auf eine schlechte Arbeit der Berater hin. In vielen Fällen liegt die Ursache in **ungenauen Vorgaben**, in Mißverständnissen oder in einer völlig unkritischen Übernahme der Vorschläge. „Da beißt sich die Katze in den Schwanz" wurde einem unserer Prüfer von einem Behördenleiter vorgehalten: „Ich hole mir den Berater doch gerade deshalb ins Haus, weil bei uns keiner Ahnung von der Technik hat; wer von uns soll denn die Frage klären, ob der verstanden hat, was wir von ihm wollen und das Ergebnis seiner Arbeit überprüfen?"

Das Dilemma ist in der Tat nicht so einfach zu beheben, allerdings ist es auch nicht ganz neu. Auch bei der Planung und Realisierung von öffentlichen Gebäuden, von Klärwerken, Straßen usw. befinden sich gerade die kleineren Verwaltungsbehörden in der Situation, daß sie sich nicht auf die Vorschläge eines einzelnen Beraters verlassen können. Sofern ihnen nicht Normen und Standards bzw. Vergleichsobjekte zur Verfügung stehen, bedarf es bis zu einem gewissen Grade des eigenen Sachverstandes oder aber der Einschaltung einer Art von „**Prüfstatiker**".



Dies wird natürlich teuer. Deshalb schlagen wir den Behörden im Lande immer und immer wieder die gemeinsam von mehreren Organisationseinheiten getragene Entwicklung von **IT-Musterlösungen** vor. Einen ersten, allerdings dornenreichen Einstieg in diese Vorgehensweise hat das Innenministerium mit der Gestaltung der IKOTECH-Arbeitsplätze vollzogen. Trotz vieler Rückschläge in den vergangenen Jahren ist ein De-facto-Standard entwickelt worden, der die Risiken für die einzelne Behörde heute weitgehend behebt. Im kommunalen Bereich ist man noch lange nicht so weit. Es ist zu hoffen, daß sich die Automationskommission der kommunalen Landesverbände auch dieser Problematik kurzfristig annehmen wird (vgl. Tz. 6.2).

Was ist zu tun?
Blindes Vertrauen in die Vorschläge von externen Beratern bei der Planung von IT-Systemen sollte ersetzt werden durch einen kritischen Dialog und den Vergleich mit Musterlösungen.

6.6 Wird der Siegeszug der Informationstechnik zu einem Waterloo für die Revisionsfähigkeit der Verwaltungsabläufe?

Die neuen Informationssysteme führen dazu, daß sich das Verwaltungshandeln mehr und mehr „im Computer abspielt". Die papierenen Akten verlieren im gleichen Maße ihre Funktion als Grundlage für Kontrollmaßnahmen. Noch fehlen verbindliche Protokollierungsregelungen für IT-Systeme.

Das Datenschutzrecht hat auf die bisherigen Erscheinungsformen der personenbezogenen Datenverarbeitung mit zwei Grundforderungen reagiert:

- Die Verarbeitungsprozesse müssen dem geltenden Recht entsprechen.
- Sie müssen so gestaltet sein, daß eine unbefugte bzw. mißbräuchliche Nutzung der Daten mit einem hinreichenden Maß an Sicherheit ausgeschlossen werden kann.

Nur wenige gesetzliche Bestimmungen wie z. B. die Pflicht zur Protokollierung von Dateneingaben und -übermittlungen und die Pflicht zur Dokumentation automatisierter Verfahren bringen den Aspekt der **Revisionsfähigkeit des Verwaltungshandelns** ins Spiel. Das hat historische Gründe. Solange sich das

Datenschutzrecht lediglich auf die Regelung der dateimäßigen Datenverarbeitung beschränkte, unterstellte es de facto eine Zweischichtigkeit der Datenbestände. Es gab die Originaldaten in den Akten und die „Arbeitsbestände" in Dateien. Wurde das Verwaltungshandeln einer aufsichtsbehördlichen oder richterlichen Kontrolle unterzogen, ließ man sich die Akte vorlegen; was darin dokumentiert war, galt als authentisch.

Hier tritt seit einigen Jahren mit zunehmender Geschwindigkeit ein gravierender Wandel ein. Die neuen Verfahren sind nicht nur bei weitem komplexer als alles, was bisher realisiert wurde, sie sind auch dadurch gekennzeichnet, daß immer mehr Teile des Verwaltungshandelns sich nur noch in den **elektronischen Datenspeichern** der Rechnersysteme nachvollziehen lassen. In diesem Zusammenhang sind insbesondere die neuen Verfahren der Justizverwaltung (MEGA, MESTA, automatisiertes Grundbuch), der Polizei (INPOL-Neu, COMPAS), der Katasterverwaltung (ALK, ALB), der Steuerverwaltung (FISKUS), der Kommunen (EIS, FIS) und der Umweltverwaltung (Umweltinformationssysteme) zu nennen. Auf den Punkt gebracht: Wer in diesen Bereichen künftig wissen will, was zu einem zurückliegenden Zeitpunkt über eine bestimmte Person wo bekannt war, wird diese Frage bestimmt nicht nach Aktenlage beantworten können.

Dies mag ein einfaches Beispiel verdeutlichen. Immer mehr Behörden gestatten ihren Mitarbeitern, innerhalb der Behörde, aber auch mit anderen Behörden per **elektronischer Post** (E-Mail) zu kommunizieren. Das bedeutet, daß Informationen in einem PC erzeugt und auf einen anderen PC übertragen werden. Sie können sowohl beim Absender wie auch beim Empfänger zu jedem beliebigen Zeitpunkt „rückstandsfrei" gelöscht werden, so daß die Tatsache der Datenübermittlung dann nicht mehr nachvollziehbar ist. Andererseits können die Daten aber auch in den PC endlos gespeichert bleiben, ohne daß aus der Akte hervorgeht, daß weitere Informationen zum betreffenden Vorgang vorliegen und wo sie sich befinden.

Überträgt man diesen Effekt auf die ins Haus stehenden großen Informationssysteme, läßt sich ermessen, welche Bedeutung die Forderung nach einer **umfassenden Revisionsfähigkeit** automatisierter Verfahren in Zukunft erlangen wird. Werden insoweit nicht stringente Protokollierungs- und Dokumentationsvorschriften erlassen, ist letztlich die Rechtswegegarantie des Art. 19 Abs. 4 Grundgesetz gefährdet. Denn diese setzt voraus, daß der Bürger überhaupt eine Chance hat, sich über die mögliche Verletzung seiner Rechte zu informieren.

In die Überlegungen zur Novellierung der Datenschutzgesetze wird man folgenden Gedanken mit einfließen lassen müssen: Eine Speicherung personenbezogener Daten ausschließlich in automatisierten Dateien ist nur zu akzeptieren, wenn **alle Aktivitäten** der technischen Systeme, die den Zugriff auf die betreffenden Daten realisieren, **protokolliert** werden und die Systeme selbst detailliert **dokumentiert** sind. Außerdem müssen die Möglichkeiten der digitalen Signatur genutzt werden, damit die Protokolldaten unverfälschbar sind und sicher zugeordnet werden können.

Dieses wird zwar zu sehr umfangreichen Protokollbeständen führen. Jedoch nur die Vollständigkeit der Protokollierung und die **strikte Zweckbindung** der Daten zu Revisionszwecken wird gewährleisten, daß elektronisches Verwaltungshandeln auch bezogen auf den Einzelfall wirklich transparent gemacht werden kann. Leider sind diese Überlegungen in die Konzeption der o. a. neuen Informationssysteme bisher nur unzulänglich eingeflossen.

Was ist zu tun?
Die zur Zeit in der Entwicklung befindlichen elektronischen Informationssysteme dürfen von den verantwortlichen Stellen nur dann zum Einsatz freigegeben werden, wenn ihre Revisionsfähigkeit durch umfassende Dokumentations- und Protokollierungsmaßnahmen gewährleistet wird.

6.7 Kontrollen im Bereich der automatisierten Datenverarbeitung

6.7.1 Zögerliche Behebung von Sicherheitsmängeln in einem Kreiskrankenhaus

Selbst die landesweite Publizität aufgrund der im letzten Jahr festgestellten gravierenden Mängel haben die Leitung und den Träger eines Kreiskrankenhauses nicht zu einer unverzüglichen und konsequenten Behebung der Schwachstellen bewogen. Angeblicher Grund: die finanziellen Rahmenbedingungen.

Die im 19. Tätigkeitsbericht (Tz. 6.6.2) dargestellten Mängel im Kreiskrankenhaus Elmshorn haben in der Öffentlichkeit und in der Presse eine breite kritische Resonanz hervorgerufen. Da die Krankenhausleitung und der Kreis Pinneberg als Träger der geprüften Stelle die **datenschutzrechtlichen Beanstandungen** weitestgehend als berechtigt **akzeptiert** haben, hätte man also erwarten können, daß kurzfristig für Abhilfe gesorgt worden wäre.

Leider ist dies nicht der Fall. In einer ersten Stellungnahme machte das Kreiskrankenhaus geltend, daß die geforderten EDV-technischen und organisatorischen Maßnahmen nicht nur differenzierte, sorgfältige interne Überlegungen und Abstimmungsprozesse voraussetzen, sondern auch die Einbeziehung des Softwarehauses erfordern würden. Dabei müßten auch die **finanziellen Rahmenbedingungen** im Krankenhausbereich berücksichtigt werden. Bei jedem Kritikpunkt sei abzuwägen, was zwingend erforderlich und was wünschbar, aber vor diesem finanziellen Hintergrund nicht kurzfristig machbar sei.

Dieser „Auslegung" der datenschutzrechtlichen Bestimmungen haben wir widersprochen und darauf hingewiesen, daß datenschutzrechtlich bedenkliche Zustände gerade in einem Bereich, der einem besonderen Berufs- und Amtsgeheimnis unterliegt, unverzüglich behoben werden müßten. Das gelte insbesondere für Maßnahmen, die keine größeren finanziellen Investitionen, sondern lediglich **organisatorische Neuregelungen** oder die Nutzung bereits bestehender technischer Möglichkeiten bedingen. Auf unsere detaillierten Fragen nach dem Stand der Arbeiten zur Umsetzung unserer Vorschläge zur Verbesserung des Daten-

schutzes erhielten wir ein Jahr nach Durchführung der Prüfung lediglich einen weiteren Zwischenbericht. Ihm ist zum Beispiel zu entnehmen:

- daß die automatisierte Datenverarbeitung nach wie vor noch nicht durch konkrete Dienstanweisungen geregelt ist,
- daß der Zugang zum Krankenblattarchiv noch nicht hinreichend abgeschottet und das Archiv personell unterbesetzt ist,
- daß Mitarbeiter der Systemadministration wie bisher auf medizinische „Echtdaten" zugreifen können,
- daß nichtanonymisierte Patientendaten als Testbestände benutzt werden,
- daß noch immer nicht geklärt ist, wer innerhalb des Krankenhauses für welche Datenbestände die Verantwortung trägt und
- daß die Patientenstammdatensätze wie bisher unbegrenzt im Krankenhausinformationssystem gespeichert bleiben, obwohl die papierenen Akten als authentischer Datenbestand angesehen werden.

Vor diesem Hintergrund stellt sich die Frage, ob es überhaupt einen Sinn macht, dem Krankenhaus wiederholt unsere Beratung bei der Lösung der Probleme anzubieten. Wenn finanzielle Überlegungen zum Maß aller Dinge erklärt werden, wird offensichtlich die strafrechtliche Seite der Angelegenheit außer acht gelassen. Aber noch steht die abschließende Stellungnahme des Kreises Pinneberg ja aus.

Was ist zu tun?
Es sollte endlich nach einem überzeugenden Konzept gehandelt werden. „Allgemeine Leitlinien" sind durch klare Vorgaben und konkrete aufbau- und ablauforganisatorische Maßnahmen zu ersetzen.

6.7.2 Tja, wenn's ums Geld geht

Viele fehlerhafte Verarbeitungsvorgänge und Sicherheitsrisiken resultieren aus unzureichenden Tests. Immer wieder wird behauptet, das Fehlerrisiko müsse man eingehen, Tests seien zu teuer. Das Landesbesoldungsamt hingegen ist ausgesprochen „risikoscheu". Aus gutem Grund.

Datensicherheit bedeutet auch, daß sich die datenverarbeitenden Stellen vor dem Echteinsatz ihrer automatisierten Verfahren davon überzeugen, daß sie in allen Einzelheiten so funktionieren, wie es geplant war. Diese Tests werden von vielen Behörden seit jeher nur unzulänglich durchgeführt, weil sie mühsam und personalaufwendig sind und somit viel Geld kosten (vgl. z. B. 19. TB, Tz. 6.3). Da hält man es häufig mit der fragwürdigen Erkenntnis: „*Nach jedem im Echtbetrieb gefundenen und dann ausgemerzten Fehler ist das Programm doch besser als vorher.*"

Wenn viel Geld auf dem Spiel steht, geht es offenbar auch anders. Das zeigte unsere Prüfung beim **Landesbesoldungsamt**, das mittels der automatisierten Verfahren PERS-SH und BABSY Monat für Monat viele Millionen an Gehältern, Löhnen, Versorgungsleistungen und Beihilfen auszahlt. Programmfehler hätten mithin fatale finanzielle Folgen. Das Testverfahren läuft so **perfekt** ab, als hätte das Landesbesoldungsamt aus einem Lehrbuch über Datenschutz und Datensicherheit abgeschrieben:

- Modifikationen an der bestehenden Software werden jeweils durch einen Auftrag an die Datenzentrale angewiesen.
- Die Details werden vorher in Arbeitsgruppensitzungen festgelegt, an denen Mitarbeiter des Landesbesoldungsamtes Schleswig-Holstein, des Landesbesoldungsamtes Mecklenburg-Vorpommern und der Datenzentrale Schleswig-Holstein teilnehmen. Sie werden fixiert in Ergebnisprotokollen und gelten als Bestandteil des jeweiligen Auftrages.
- Über den Test wird von der Datenzentrale und dem Landesbesoldungsamt ein gemeinsames Protokoll erstellt, aus dem sich folgende Teilaspekte ergeben: Auftragsnummer, Projekt, Testinhalt, Namen der getesteten Programme, Zeitpunkt des DZ-Tests und der Übergabe der geänderten Module an das Landesbesoldungsamt, Zeitpunkt des Abschlußtests durch das Landesbesoldungsamt, Namen der Tester der DZ, Namen der Tester des Landesbesoldungsamtes, Testergebnis, Freigabetestat („die Programme werden zur Anwendung im Rechenzentrum Altenholz freigegeben"), Unterschriften der verantwortlichen Mitarbeiter der DZ und des Landesbesoldungsamtes.
- Die Durchführung der Tests erfolgt durch sechs (!) qualifizierte Sachbearbeiter des Landesbesoldungsamtes, die jeweils auf einen unterschiedlichen Teilbereich der Verfahren spezialisiert sind. Durchschnittlich verfügt jeder Tester über einen Bestand von 600 anonymisierten Testfällen. Die ca. 3 600 (!) Testdatensätze werden kontinuierlich an die geänderte Rechtslage angepaßt.

Nach Aussage des Landesbesoldungsamtes hat diese seit Jahren praktizierte Verfahrensweise dazu geführt, daß gravierende Softwarefehler und sonstige Unregelmäßigkeiten weitestgehend vermieden wurden. Wen wundert's?

Was ist zu tun?
Zur Nachahmung empfohlen!

6.7.3 Wenn die automatisierte Datenverarbeitung wirklich Chefsache ist

Es ist selten, daß sich Behördenleiter tatsächlich für die automatisierte Datenverarbeitung in ihrem Haus verantwortlich fühlen. Ist dies der Fall, entstehen zwar nicht automatisch perfekte Lösungen, aber in der Regel führt es zu Konzepten „aus einem Guß".

Seit mehreren Jahren führen wir schwerpunktmäßig im kommunalen Bereich sicherheitstechnische Überprüfungen durch, um Schwachstellen aufzudecken, und insbesondere auch, um im konkreten Einzelfall durch Beratung zu einer Problemlösung beizutragen (vgl. 19. TB, Tz. 6.6.1). Bei den meisten dieser Prüfungsmaßnahmen finden wir vergleichbare Sachverhalte vor, einige Verwaltungen fallen allerdings „**aus dem Rahmen**", im positiven wie auch im negativen Sinne. Bemerkenswert waren z. B. im abgelaufenen Jahr die Verhältnisse in der Stadtverwaltung Plön: Hier war der „EDV-Macher" nicht – wie sonst häufig anzutreffen – ein zeitlich und fachlich überforderter Mitarbeiter im Hauptamt, der das „Geschäft" nebenbei mitzuerledigen hatte, sondern das „EDV-Team" bestand aus dem Bürgermeister selbst und dem büroleitenden Beamten sowie einem Sachbearbeiter, der die Weisungen der Entscheidungsträger umzusetzen hatte.

Während der gesamten Prüfung standen dementsprechend der **Bürgermeister** und der **Büroleiter** Rede und Antwort und konnten die Gründe für ihre Hardware-, Software- und Organisationsentscheidungen der letzten Jahre im Detail erläutern. Nicht ein einziges Mal bekam unser Prüfer die sonst übliche Antwort zu hören: „Darum habe ich mich nicht gekümmert, da müssen Sie unseren Techniker oder das Softwarehaus fragen."

Das bedeutete nicht, daß wir keine **sicherheitstechnischen Mängel** vorgefunden haben. Die schwierige Abschottung der Benutzerebene der Systeme zur Administrationsebene hatte man z. B. auch hier nicht voll in den Griff bekommen. Auch fehlte die Dokumentation der Verfahren, was fast schon verständlich war, hatten die beiden Chefs ihr Gesamtsystem doch im Kopf. Dabei handelte es sich bei ihnen durchaus nicht um EDV-Freaks, die im Dienst ihrem Hobby frönten. Es waren vielmehr gestandene Verwaltungsprofis, die nur nicht bereit waren, die Entscheidungen über den Einsatz von Informationstechnik in ihrer Verwaltung aus der Hand zu geben. Wenn sich einzelne Maßnahmen im nachhinein als nicht zweckmäßig oder sachgerecht herausstellten, wurden die Korrekturen mit der selben „Souveränität" vorgenommen, wie man die ursprünglichen Entscheidungen getroffen hatte. Entsprechend schnörkellos wurden die Beanstandungen, die aus unserer Prüfung resultierten, abgearbeitet.

Was ist zu tun?
Behördenleiter sollten sich nicht scheuen, die automatisierte Datenverarbeitung zur Chefsache zu erklären. Das hierzu erforderliche „Fachwissen" besteht zu einem großen Teil aus der Sturheit, nur verwaltungstechnisch überzeugende Lösungen zu akzeptieren und Datensicherheit als „Bringschuld" der Anbieter zu betrachten.

6.7.4 Der Inhalt eines typischen Prüfberichts

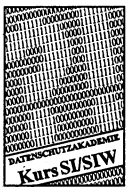
Die Diskrepanz zwischen den gesetzlichen Anforderungen und der Wirklichkeit in bezug auf die Datensicherheit und die Ordnungsmäßigkeit der Datenverarbeitung ist gravierend. Das zeigen immer wieder die im Rahmen von Prüfungen vorgefundenen Sachverhalte. Sie müßten selbst die schärfsten Datenschutzkritiker nachdenklich stimmen.

In den Diskussionen um die Datensicherheit und die Ordnungsmäßigkeit der personenbezogenen Datenverarbeitung in der Verwaltung wird uns immer wieder vorgehalten, unsere Forderungen seien zu puristisch und berücksichtigten nicht die „Sachzwänge der Praxis". Es erscheint daher angebracht, einmal transparent zu machen, welche Sachverhalte wir typischerweise bei unseren Prüfungen vorfinden. Bei dem nachfolgenden Text handelt es sich um einen lediglich redaktionell gekürzten wörtlichen Auszug aus dem Abschnitt „**Einzelfeststellungen**" einer **Prüfungsniederschrift**:

- Ablauforganisatorische Regelungen konnten nicht vorgelegt werden. Ein IT-Konzept, das die **Vorgaben** für die Entwicklung der Hard- und Software beschreibt, besteht nicht. Dienstanweisungen für den Betrieb der EDV-Systeme sowie für die Systembetreuer wurden nicht erstellt.
- Besondere **Zugangsregelungen** für die Server im Bau- und Sozialamt wurden nicht getroffen. Sie sind nicht in gesicherten Räumen, sondern unmittelbar in den Mitarbeiterbüros installiert.
- Die **Administration** der Hard- und Software wird zum Teil von den jeweiligen Mitarbeitern der Fachabteilungen durchgeführt. Bei technischen Schwierigkeiten werden im Einzelfall Fremdleistungen von externen Dienstleistungsfirmen in Anspruch genommen. Eine Kontrolle der Dienstleister wird nicht durchgeführt.
- Die von den Fachämtern verarbeiteten Daten werden überwiegend auf den **Einzelplatz-PC** gespeichert. Eine Anweisung, die den Umgang mit personenbezogene Daten regelt, existiert nicht.
- Im **zentralen Schreibdienst** sind auf einem PC über 2 000 Dokumente festgestellt worden. Das älteste Dokument wurde am 27.10.1992 zuletzt bearbeitet, das ist vermutlich der Zeitpunkt, an dem der PC erstmalig zum Einsatz gelangte. Eine ähnliche Situation wurde auf dem PC im Vorzimmer des Bürgermeisters vorgefunden. Auch hier konnten 2 597 zum Teil sehr brisante Dokumente aus folgenden Bereichen festgestellt werden: Sitzungsdienst, Protokolle (834 Dokumente), Vorlagen für den Sitzungsdienst (648 Dokumente), Schriftverkehr des Bürgermeisters (1 097 Dokumente).
- Die **Löschung** der Daten wird nicht durch die Fachvorgesetzten angewiesen. Die Mitarbeiter verwalten ohne Kontrolle der verantwortlichen Ebene die Daten nach eigenem Ermessen.

- Die Löschung der nicht mehr benötigten Daten ist aufgrund der **unstrukturierten Speicherverwaltung** sehr umständlich.
- Die inhaltliche **Kontrolle** der gespeicherten Daten ist durch die Fachvorgesetzten **kaum möglich**. Die Benutzer sind somit in der Lage, Datenbestände aufzubauen, ohne daß die Amtsleitung die Erlaubnis hierzu erteilt hat.
- Die **Datensicherung** auf den PC und den Servern liegt in der Verantwortung der Benutzer. Die Art und Weise der Durchführung der Datensicherung wurde jedoch nicht geregelt. Zum Beispiel wird im Vorzimmer des Bürgermeisters die Datensicherung nur unregelmäßig von der Sekretärin durchgeführt. In anderen Fachbereichen wurden vergleichbare Gegebenheiten festgestellt.
- Eine **Dokumentation** über die berechtigten PC-Benutzer und die ihnen zugewiesenen Rechte konnte nicht vorgelegt werden. Im Bereich des Bauamtes wurden die Benutzerrechte auf dem Server von dem Lieferanten offenbar ohne Weisung des Fachamtsleiters eingerichtet. Die Supervisor-Kennung war dem Systembetreuer des Bauamtes nicht bekannt. Es konnte deshalb nicht festgestellt werden, welche Benutzer eingerichtet und welche Rechte zugewiesen wurden. Ebensowenig konnte geklärt werden, für welche konkreten „dienstlichen" Aufgaben der Server im einzelnen eingesetzt wurde.
- Es wurden folgende **Mängel** in der **technischen Konfiguration** der Arbeitsstationen und der Server festgestellt: Die Benutzer haben Zugriff auf die Betriebssystemebene ihrer Arbeitsstationen und der Server. Die Diskettenlaufwerke sind für den Datenaustausch offen. Auf den Arbeitsstationen befindet sich umfangreiche Software, die nicht zur Ausführung der für das betreffende Gerät zugelassenen Verfahren erforderlich ist. Auf den Arbeitsstationen ist die Windows-Oberfläche durch die Benutzer veränderbar. Beispielsweise ist das Entfernen oder Hinzufügen neuer Programmgruppen möglich. Zugriffsrechte können auf den Arbeitsstationen aufgrund fehlender Sicherheitssoftware nicht anwenderbezogen erteilt werden. Aufgrund dieser Gegebenheiten ist nicht ausgeschlossen, daß Daten unbefugt verändert oder gelöscht werden, ein Virenangriff erfolgreich wäre, Daten außerhalb eines zugelassenen Verfahrens gespeichert, Daten auf Disketten kopiert und für andere Zwecke verwendet, Zuständigkeiten für bestimmte Aufgaben nicht erkannt werden, die Server bei auftretenden Fehlern für längere Zeit ausfallen.
- Für keines der eingesetzten Verfahren wurde bislang eine Dokumentation, bestehend aus einer **Aufgabenbeschreibung**, einer **Programm- und Verfahrensbeschreibung** sowie **Test- und Freigabeunterlagen** erstellt. Es konnte keine Bestandsliste für die verwendeten Programme und Verfahren vorgelegt werden.
- Für die **EDV-Systeme** wurde keine Zusammenstellung über die in der Verwaltung eingesetzte Hardware erstellt.
- Die durchgeführten Systemarbeiten werden nicht in einem System-Logbuch „protokolliert". Bei Hardwarestörungen administrieren auch Techniker von **Dienstleistungsfirmen** die Systeme. Diese Systemarbeiten werden ohne Aufzeichnungen ausgeführt. Es ist deshalb nicht feststellbar, zu welchem Zeitpunkt welche Personen welche Arbeiten durchgeführt haben.

- **Schulungen** auf dem Gebiet des Datenschutzrechts, insbesondere zur Umsetzung von gesetzlichen Regelungen in konkrete technische und organisatorische Maßnahmen, wurden nicht durchgeführt.



Diese Ergebnisse sprechen unseres Erachtens für sich. Es muß nochmals betont werden, daß es sich um übliche Prüfungsergebnisse handelt, die im vergangenen Jahr in ähnlicher Form mehr als einem halben Dutzend Behörden „ins Stammbuch geschrieben" werden mußte. Daß derartige Gegebenheiten nicht unbeanstandet bleiben können, dürfte ebenso einleuchten wie die nachdrückliche Forderung nach einer unverzüglichen Behebung der Mängel.

Was ist zu tun?
Solange eine derartige Diskrepanz zwischen den gesetzlichen Anforderungen an die Datensicherheit und die Ordnungsmäßigkeit der personenbezogenen Datenverarbeitung und der Realität besteht, muß den Überprüfungen und Beratungen vor Ort weiterhin eine hohe Priorität beigemessen werden.

6.7.5 Wer überwacht die Fernwartung?

Den Fernwartungsunternehmen wird oft blindes Vertrauen entgegengebracht, obwohl deren Aktivitäten sich im sensibelsten Bereich eines Computersystems vollziehen. Bindende Sicherheitsvorschriften werden dabei mißachtet.

Der Zugang zur Betriebssystemebene eines Computers ist unter sicherheitstechnischen Aspekten zu vergleichen mit der Übergabe der Verfügungsgewalt über den **Tresorschlüssel** einer Bank. Diese Erkenntnis hat ihren Niederschlag auch in der von der Landesregierung im Jahr 1994 erlassenen Datenschutzverordnung (DSVO) gefunden.

Im Wortlaut: § 9 Abs. 1 DSVO
Durch technische und organisatorische Maßnahmen ist sicherzustellen, daß verändernde Zugriffe auf Programme zur Systemsteuerung und auf freigegebene Anwendungsprogramme und Verfahren nur durch dazu ausdrücklich befugte Personen erfolgen können und diese durch weisungsbefugte Mitarbeiterinnen oder Mitarbeiter oder deren Beauftragte kontrolliert werden. Dies gilt nicht für Personen, die informationstechnische Geräte ausschließlich in eigener Verantwortung betreiben.

Die Gründe hierfür liegen auf der Hand und sind in ausführlichen Hinweisen im Amtsblatt 1994, Seite 140, dargelegt worden. Wer auf die **Betriebssystemebene** eines Computers gelangt, kann nämlich meist „ohne **Fingerabdrücke** zu hinterlassen", Daten löschen, Daten hinzufügen, Daten inhaltlich verändern, Protokollbestände modifizieren, Benutzerrechte erweitern und die Verarbeitungslogik von Programmen beeinflussen. Dies alles kann erforderlich und sinnvoll sein, es kann aber auch versehentlich und ungewollt passieren, letztlich sind auch Absicht und kriminelle Energie nicht auszuschließen. Auch die Konsequenzen sind höchst unterschiedlich. In dem einen Fall werden fehlerhafte Systemzustände

korrigiert. In dem anderen Fall Ergebnisse verfälscht, Daten unbefugt offenbart oder wichtige Informationen unwiederbringlich vernichtet.

Bei der **Systemadministration** handelt es sich also um eine so wichtige **Schlüsselfunktion**, daß sie kein EDV-Verantwortlicher ohne Grund aus der Hand geben dürfte. Was aber, wenn man selbst nicht über die Kenntnisse verfügt, die erforderlich sind, um ein kompliziertes Computersystem zu steuern? Man kauft sich das nötige Know-how bei einem externen Dienstleister ein. Und damit der nicht bei jeder Kleinigkeit ins Haus kommen muß, vereinbart man eine sogenannte Fernwartung. Über eine Telefonleitung werden dabei der Computer der Behörde und der des Wartungsunternehmens zusammengeschaltet, und der Dienstleister kann alle Systemsteuerungsaktivitäten vom eigenen Schreibtisch aus vollziehen.

Da stellt sich natürlich das Problem der Überwachung durch die Behörde. Wie nachlässig dabei verfahren wird, haben in jüngster Zeit mehrere Prüfungen gezeigt. Selbst bei **Fernwartungen** durch die **Datenzentrale** waren die Sicherheitsmängel so gravierend, daß sie in diesem Bericht nicht alle detailliert dargestellt werden können. Es ist nicht auszuschließen, daß sie bei einigen Behörden nach wie vor bestehen und eine Publizierung zu unvertretbaren Risiken führen würde. Daher nur ein Auszug aus der **Mängelliste**:

- Schriftliche Verträge mit verbindlichen Leistungsbeschreibungen und Sicherheitskonzepten bestanden nicht.
- Es erfolgte nicht nur die Behebung technischer Fehler, sondern auch die Behebung von Mängeln in der Software, die sich bereits im Echteinsatz befand.
- Teilweise wurden sogar die Datenbestände inhaltlich korrigiert.
- Die Systemadministratoren hatten wegen anderweitiger Aufgaben keine Zeit, die Arbeiten der Datenzentrale zu überwachen.
- Es wurden zwar Protokolle erstellt, für die Behörden waren sie jedoch mangels entsprechender Kenntnisse nicht lesbar.
- Die Notwendigkeit der Systemzugangs ergab sich so häufig (110mal in 50 Arbeitstagen, teilweise 6mal an einem Tag), daß die Zugangsmöglichkeit für die Datenzentrale (z. B. durch Abschalten des Modems) über längere Zeiträume gar nicht unterbrochen wurde.
- In der Datenzentrale waren mehrere und häufig wechselnde Personen mit der Fernwartung des betreffenden Rechnersystems betraut. Das Zugangspaßwort war allen Mitarbeitern bekannt. Die Paßworte für alle Fernwartungskunden wurden nach dem gleichen einfachen Algorithmus generiert.

Zusammengefaßt kann festgestellt werden, daß sowohl die betreffenden Behörden wie auch die Datenzentrale massiv gegen die datenschutzrechtlichen Sicherheitsbestimmungen verstoßen haben. Alle Beteiligten haben dies eingesehen und Besserung gelobt. Ob sie dies auch einhalten, werden die nächsten Prüfungen zeigen.

Was ist zu tun?
Behörden, die Fernwartungen oder andere Wartungsmaßnahmen von externen Dienstleistern durchführen lassen, sollten ihre Verfahrensweisen kritisch überprüfen. Auf eine Überwachung der Wartungsarbeiten kann in keinem Fall verzichtet werden.

6.7.6 Noch immer nicht alle Sicherheitsprobleme im IKONET/Campus-Netz gelöst

Gerade wenn Ministerien über Computersysteme miteinander kommunizieren wollen, müssen hinreichend sichere sicherheitstechnische Rahmenbedingungen geschaffen werden. Dies kann nicht gewährleistet werden, wenn sich niemand als Netzbetreiber verantwortlich fühlt.

> ? *Campus-Netz*
>
> *Bei dem Campus-Netz handelt es sich um die Weiterentwicklung des IKONET. Es verbindet die lokalen Rechnernetze der Ministerien, der Staatskanzlei und des Landtages auf der Basis einheitlicher Konventionen.*

Die Überprüfung der Sicherheitskomponenten im internen Datennetz der Landesregierung hat bereits im Oktober 1996 stattgefunden. Auf die Grundsatzprobleme und die Sicherheitslücken haben wir im Dezember 1996 schriftlich hingewiesen (vgl. 19. TB, Tz. 7.9). Im abgelaufenen Jahr sind zwar im Detail sicherheitstechnische Verbesserungen vorgenommen worden. Die **grundsätzlichen Problemstellungen** wurden aber noch immer nicht angepackt. Der Grund hierfür liegt darin, daß nach wie vor Unklarheit darüber besteht, wer als der verantwortliche Betreiber des Netzes anzusehen ist. Zudem bestreitet das Innenministerium, daß es sich bei dem Netz um ein automatisiertes Verfahren im Sinne des Datenschutzrechts handelt.

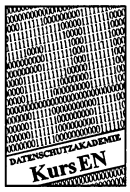
Die **Verantwortungsfrage** ist nach unserer Auffassung vorrangig zu klären (vgl. hierzu auch Tz. 6.7.7). Wenn ein Ministerium sich entscheidet, z. B. personenbezogene Daten über dieses Netz in ein anderes Ministerium zu übertragen, muß es wissen, welche Sicherheitsmaßnahmen unterwegs greifen. Bevor der Ministeriumscomputer mit dem Netz verknüpft wird, um über das Internet mit der Welt zu kommunizieren, muß geklärt sein, welche Abschottungen die Netz-Firewall übernimmt und welche Aktivitäten man selbst ergreifen muß, um zu verhindern, daß „**angriffslustige Hacker**" nachweisen, wie man Behördenrechner manipulieren kann. Wenn der Zugang zu externen Netzen nur über einen einzigen, gesicherten Ein- und Ausgang erfolgen soll, müssen sich alle Teilnehmer verpflichten, keine eigenen Öffnungen einzurichten.

Wer definiert aber diese Regeln, und wer überwacht ihre Einhaltung? Vor allem wer entscheidet, ob sich alle Teilnehmer „netzkonform" verhalten, und wer möglicherweise wegen der Verletzung der „Spielregeln" von der Netzbenutzung ausgeschlossen wird? Wer definiert und erweitert kontinuierlich die einzelnen Filterfunktionen der Firewalls an der Schnittstelle zum Internet, und wer testet die gewünschte Funktionsweise dieser von externen Softwarehäusern generierten Software? Wer gewährleistet letztlich die Ordnungsmäßigkeitskriterien der Datenschutzverordnung (Sicherheitskonzept, Dokumentation, Test, Freigabe, Administrationsüberwachung usw.)? Zur Zeit geschieht dies alles auf der Basis einer lockeren interministeriellen Zusammenarbeit der IT-Leitstellen. Das Innenministerium schafft Regelungen für das eigene Haus und gibt sie den IT-Leitstellen der anderen Ressorts mit der Anregung zur Nachahmung weiter. Die Verantwortung für das Datennetz tragen die beteiligten Ministerien also praktisch „**zur gesamten Hand**" bzw. nach der Devise „Vertrauen gegen Vertrauen".

Es wird zudem bestritten, daß im Campus-Netz personenbezogene Datenverarbeitung stattfindet. Das Netz sei nur die technische Voraussetzung für die gesondert zu betrachtenden **Verarbeitungsprozesse**, vergleichbar der Strom-, Wasser- und Wärmeversorgung. Diese Auffassung verkennt, daß ein solches Netz Hard- und Softwarekomponenten enthält, die so modifizierbar sind, daß die Ergebnisse der Verarbeitung beeinflußt werden. Niemand käme beispielsweise auf die Idee, den Botendienst eines Ministeriums aus den Sicherheitsüberlegungen auszublenden, weil die Mitarbeiter in diesem Bereich keine Daten „verarbeiten", oder das Innenministerium aus der datenschutzrechtlichen Pflicht zu entlassen, die gemeinsame Telefonanlage der Ministerien und des Landtages so zu konfiguieren, daß z. B. das Fernmeldegeheimnis der Abgeordneten gewährleistet wird.

Wir haben deshalb das **Innenministerium** nochmals darauf aufmerksam gemacht, daß

- die Entscheidungen über die Anwendung von Verschlüsselungstechniken,
- die Aktivitäten zur Virenabwehr und zur Abwehr „aktiver Inhalte",
- die Maßnahmen zur Vermeidung des unbeabsichtigten Absendens von Dokumenten,
- die Vorkehrungen zum Ausschluß einer programmgesteuerten Auswertbarkeit der zwischengespeicherten Daten,
- die Fortentwicklung und Optimierung der Firewalls usw.



nur in einem definierten und dokumentierten Abstimmungsprozeß zwischen allen Ressorts **verbindlich** festgemacht werden können. Das gleiche gilt für die Frage, ob die Fortentwicklung des Netzes künftig der Datenzentrale im Wege der Auftragsdatenverarbeitung übertragen werden kann. Nach unserer Auffassung sind schriftliche und bindende Vereinbarungen unverzichtbar.

Was ist zu tun?
Alle Beteiligten müssen sich an einen Tisch setzen, eine „Netzgeschäftsordnung" definieren, gemeinsam die Sicherheitslücken schließen und ein verantwortliches und weisungsberechtigtes Ressort „küren". Dies liegt im Interesse aller Beteiligten und ist datenschutzrechtlich unverzichtbar.

6.7.7 Nachbesserungen im Schleswig-Holstein-Netz – „nur auf freiwilliger Basis"?

Der Datenzentrale fällt es schwer, ihr Schleswig-Holstein-Netz als „normales" automatisiertes Verfahren zu betrachten. Sie reklamiert hierfür einen Sonderstatus und will das „zu strenge" Datenschutzrecht nur analog anwenden.

Im Tätigkeitsbericht für das Jahr 1996 haben wir von der Datenzentrale gefordert, das von ihr betriebene **Schleswig-Holstein-Netz** sicherheitstechnisch nachzubessern und die Datensicherheitsmaßnahmen zu dokumentieren. Ihre Kunden haben wir aufgefordert, darauf zu achten, daß in den Nutzungsverträgen das erforderliche Sicherheitsniveau festgeschrieben ist (vgl. 19. TB, Tz. 7.8).

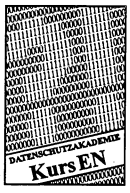
Wie berechtigt unsere Forderungen waren, machte die Prüfung bei einer größeren Kommune deutlich, die den Datentransfer in das **Rechenzentrum der Datenzentrale** über das Schleswig-Holstein-Netz abwickelt. Zum Zeitpunkt der Prüfung (März 1997) stellte sich die Situation dort wie folgt dar: Die Datenzentrale hatte der Stadtverwaltung die Nutzung des Schleswig-Holstein-Netzes mit den Argumenten angeboten, es werde bereits von mehr als 80 Kunden benutzt; es erfülle vor allem die Anforderungen der öffentlichen Verwaltung an Datensicherheit und Datenschutz; in den Netzknoten seien Komponenten der DZ installiert, die von ihr selbst administriert und gewartet würden; der besondere Vorteil des Schleswig-Holstein-Netzes liege in der Geschlossenheit, die als Basis für den Datenschutz und die Datensicherheit eine günstige Voraussetzung biete.

Die Inanspruchnahme des Netzes erfolgte daraufhin **ohne weitere Prüfung**. Ein schriftlicher Vertrag zwischen der DZ und der Stadtverwaltung wurde nicht geschlossen. Das Verfahren ist bezüglich der Sicherheitskriterien nicht getestet und freigegeben worden. Die Stadtverwaltung wurde von der DZ zum Beispiel nicht über den Ort des Einwahl- bzw. Netzknotens, die Konfiguration der Leitungen für die Datenkommunikation, die Abschottung der Daten vor unbefugten Zugriffen auf dem Übertragungswege sowie die Absicherung der Netzknoten bzw. der Datenvermittlungsstellen informiert. Erst im Rahmen unserer Prüfung wurde der Kommune klar, wo sich z. B. die technischen Komponenten des Netzknotens

befinden und daß die dort getroffenen Sicherheitsmaßnahmen keineswegs den „Anforderungen an den Datenschutz und die Datensicherheit" entsprachen.

Die Datenzentrale reagierte auf diese Feststellungen mit einer an sich nicht gebotenen Gelassenheit. Zwar wurden den Kunden ab Oktober 1997 schriftliche Verträge ausgehändigt und ein Sicherheitskonzept erstellt. Insgesamt ist man allerdings, wie auch das Innenministerium bezüglich des Campus-Netzes (vgl. Tz. 6.7.6), der Auffassung, daß ein solches Netz nicht nach datenschutzrechtlichen Kriterien zu beurteilen sei, weil es sich bei dem Transport von Daten nicht um eine Datenverarbeitung im Auftrag handele. Die Daten würden nicht zweckgerichtet genutzt. Die Übertragung oder der Transport von Daten seien nur Mittel, um einen bestimmten Zweck zu erfüllen. Man sei aber gleichwohl bereit, das **Datenschutzrecht analog** anzuwenden, gleichsam auf freiwilliger Basis.

Das Datenschutzrecht kennt keinen Datentransport als Datenverarbeitung „sui generis". Deshalb können die von der Datenzentrale bedauerten „strengen Anforderungen an die Organisation einer **Auftragsdatenverarbeitung** mit schriftlichen Weisungen und den Folgen hohen Aufwandes bei Änderungen im Leistungsumfang oder in den Abläufen" nicht dazu führen, daß das Datenschutzrecht auf das Schleswig-Holstein-Netz nur auf freiwilliger Basis angewendet wird. Im Vordergrund der Betrachtungen muß vielmehr das Rechtsverhältnis zwischen den Betroffenen und den datenverarbeitenden Stellen stehen. Wenn sich eine Behörde aus ökonomischen Gründen entscheidet, Teile des Verarbeitungsprozesses in die Hände externer Dienstleister zu geben, muß durch konkrete Weisungen in schriftlichen Verträgen und durch entsprechende Kontrollmaßnahmen gewährleistet werden, daß das datenschutzrechtlich gebotene Sicherheitsniveau auch außerhalb der unmittelbaren Einflußsphäre der verantwortlichen Stelle gewahrt wird.



Was ist zu tun?
Datenschutz wird nicht zur reinen Gefälligkeit, wenn dem Dienstleister die Daten zur Auftragsdatenverarbeitung über ein eigenes Netz übermittelt werden. Dies muß die Datenzentrale akzeptieren.

7. Neue Medien und Informationstechniken

7.1 Vorbildliche Regelung des Datenschutzes bei Multimedia

Die neuen Multimediagesetze regeln den Datenschutz eigentlich vorbildlich. Allerdings stehen wichtige Schutzvorschriften unter dem Vorbehalt, die datenschutzfreundliche Lösung müsse „technisch möglich und zumutbar" sein. Hier besteht Bedarf für Überzeugungs- und Umsetzungsarbeit.

Am 01.08.1997 sind die neuen Regelungswerke zum Multimediabereich in Kraft getreten. Das **Informations- und Kommunikationsdienstegesetz** (IuKDG) des Bundes gilt für die Teledienste, bei denen die Individualkommunikation im Vordergrund steht, und der **Mediendienste-Staatsvertrag** (MDStV) der Länder regelt das Recht der Mediendienste, bei denen die Informationsverteilung in ähnlichen Strukturen verläuft wie bei Rundfunk und Presse (sog. One-to-Many-Struktur). Bund und Länder konnten sich nicht endgültig über die genaue Grenzziehung ihres Zuständigkeitsbereiches einigen.

> **?** ***Multimediadienste***
>
> *Mediendienste sind an die Allgemeinheit gerichtet; bei ihnen steht die redaktionelle Gestaltung zur Meinungsbildung im Vordergrund. Sie können als rundfunkähnliche Verteildienste, aber auch als Abrufdienste vorkommen. Wie Rundfunk und Presse unterfallen sie der Regelungskompetenz der Länder. Beispiele: Fernseheinkauf, elektronische Presse, Teletext.*

Als pragmatischer Kompromiß wurden weitgehend gleichlautende Regelungen für den jeweiligen Zuständigkeitsbereich geschaffen. Die Datenschutzvorschriften des IuKDG finden sich im Teledienstedatenschutzgesetz (TDDSG), die des MDStV in den dortigen §§ 12-17.

Die neuen **Datenschutzregelungen** können als **vorbildlich** angesehen werden. Sie könnten ein Modell für den Datenschutz der dritten Generation bilden, denn sie regeln in überschaubarer und leicht lesbarer Weise, welche Datenverarbeitung bei den Diensteanbietern, z. B. im Internet, zulässig ist. Dabei setzen die Vorschriften bereits einige Vorgaben um, die aufgrund der EG-Richtlinie zum Datenschutz im gesamten deutschen Datenschutzrecht bis zum Herbst 1998 Berücksichtigung finden müssen. Sie kommen daher zu einem Datenschutzniveau, das deutlich über dem des Bundesdatenschutzgesetzes liegt.

> **?** ***Teledienste***
>
> *Bei den Telediensten steht die individuelle Nutzung im Vordergrund. Für diese Materie liegt die Regelungskompetenz beim Bund. Beispiele: elektronischer Datenaustausch, Videokonferenzen, Angebote zur Nutzung des Internet, Online-Kaufhäuser mit sofortiger Bestellmöglichkeit, Telebanking, Telemedizin, Telespiele.*

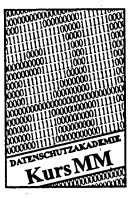
Im einzelnen sind folgende Regelungen hervorzuheben:

- Die Dienste sind von vornherein so zu gestalten, daß keine oder sowenig wie möglich personenbezogene Daten erhoben und verarbeitet werden. Damit ist erstmals der Grundsatz der **Datenvermeidung** und der **Datensparsamkeit** gesetzlich festgeschrieben.
- „Soweit dies technisch möglich und zumutbar ist", müssen Medien- und Teledienste so abgerechnet werden, daß der Nutzer **anonym** oder unter **Pseudonym** auftreten kann. Dadurch soll verhindert werden, daß die aus den Abrechnungsdaten erkennbar werdenden Interessen und Gewohnheiten der Benutzer bestimmten Personen zugeordnet werden können.
- Die Informationen über die Inanspruchnahme der verschiedenen Dienste dürfen nicht zusammengeführt und zu einem **Persönlichkeitsprofil** verdichtet werden. Nutzungsprofile dürfen allenfalls unter Pseudonym erstellt werden. Den gläsernen Kunden darf es demnach in bezug auf die Nutzer der Dienste nicht geben.
- Die Daten der Nutzer von Diensten dürfen ausschließlich **zweckgebunden** verwendet werden. Ursprünglich vorgesehene weitgehende Zugriffsrechte der Geheimdienste auf die Kundendateien der Anbieter wurden nach Protesten der Datenschutzbeauftragten (vgl. 19. TB, Tz. 7.2) aus dem Gesetz gestrichen. Eine Nutzung z. B. für Werbezwecke ist nur mit ausdrücklicher vorheriger Einwilligung zulässig. Dies ist besser als die Regelung im Bundesdatenschutzgesetz, nach der der Betroffene der Nutzung seiner Daten für Werbung von sich aus widersprechen muß.
- Werden Daten über Nutzer erhoben, so sind sie darüber zuvor zu **unterrichten**. Niemand soll von der Datenerhebung durch die Diensteanbieter überrascht werden.
- Es muß sichergestellt sein, daß sich der Nutzer zu jeder Zeit aus dem Tele- oder Mediendienst ausklinken und die **Verbindung abbrechen** kann. Dadurch soll gewährleistet werden, daß die Nutzer stets „das Heft in der Hand behalten".
- Sofern bei den Zugriffen der Nutzer personenbezogene Daten anfallen, sind sie sofort nach Beendigung der Inanspruchnahme der Dienste zu **löschen**, soweit sie nicht (ausnahmsweise) für Abrechnungszwecke benötigt werden.
- Es muß ausgeschlossen werden, daß **Dritte** die Inanspruchnahme von Diensten zur Kenntnis nehmen. Damit werden die schutzwürdigen Interessen der Nutzer nicht nur gegenüber den Diensteanbietern, sondern auch gegenüber anderen Nutzern gewahrt.
- Die Abrechnung darf die Inanspruchnahme der einzelnen Angebote nicht erkennen lassen, sofern der Nutzer nicht ausdrücklich einen **Einzelnachweis** verlangt. Niemand muß es hinnehmen, daß sein Nutzungsverhalten zwangsläufig durch die Gebührenrechnung publik wird.
- Die **Datenschutzaufsichtsbehörde** kann bei Telediensten nunmehr auch sogenannte **Spontankontrollen** durchführen. Nach dem herkömmlichen Datenschutzrecht für den privaten Bereich ist in den meisten Fällen eine Kontrolle

nur dann möglich, wenn konkrete Anhaltspunkte für eine Rechtsverletzung vorliegen.

Ein weiterer positiver Ansatz findet sich im MDStV, nämlich die Möglichkeit, ein **Datenschutz-Audit** durchführen zu lassen. Diese zunächst auch im IuKDG vorgesehene Möglichkeit wurde dort im Laufe der Gesetzgebung gestrichen. Allerdings ist es nicht ausgeschlossen, daß auf Bundesebene entsprechende Vorschläge erneut aufgegriffen werden. Erforderlich wäre es dann, ein Rahmengesetz zu formulieren, das ein Verfahren für die Zertifizierung von Datenschutzqualität vorgibt. Ein solches Audit könnte sich zum Verkaufsargument entwickeln, da ein Großteil der Nutzer der neuen Medien für Datenschutzbelange sensibilisiert ist.

> **? *Datenschutz-Audit***
>
> *Ein Datenschutz-Audit besteht aus einer Prüfung und Bewertung des Datenschutzkonzepts sowie der technischen Einrichtungen eines Anbieters vor Inbetriebnahme durch unabhängige Gutachter. Bei guten Ergebnissen ist die Vergabe eines Gütesiegels denkbar.*



Der Wortlaut der Multimediagesetze regelt den Datenschutz der Nutzerinnen und Nutzer also in vorbildlicher Weise. Der wirkliche Nutzen der Gesetze steht und fällt aber mit ihrer **praktischen Umsetzung**. Dabei muß sich zeigen, ob die Formulierung „technisch möglich und zumutbar" eine Hintertür öffnet, die den Vorteil der Gesetze für die Bürgerinnen und Bürger in Frage stellt.

Was ist zu tun?
Die Diensteanbieter und Nutzerorganisationen sollten sich zusammen mit den Datenschutzbeauftragten überlegen, welche datenschutzfreundlichen Technologien „technisch möglich und zumutbar" sind und sie realisieren.

7.2 Signaturgesetz und -verordnung

Das Signaturgesetz ist in Kraft getreten. Sobald die Details der Verfahren für die digitale Signatur in der Signaturverordnung und in den Ausführungsbestimmungen festgelegt sind, kann man elektronisch unterschreiben und Texte gegen Manipulation schützen.

Die **digitale Signatur** dient als eine Art persönliches Siegel für elektronische Dokumente und soll ein Unterzeichnen ähnlich der **Unterschrift** auf dem Papier ermöglichen. Damit können rechtsverbindliche Verträge auch über Datennetze fälschungssicher geschlossen und vertrauliche personenbezogene Daten sicher vor unerkennbarer Veränderung übermittelt werden. In künftigen Gesetzen kann die elektronische Unterschrift auch dort zugelassen werden, wo heute rechtlich bestimmte Formerfordernisse bestehen.

Grundlage für die digitale Signatur sind kryptographische Verfahren, die mit einem **Schlüsselpaar** arbeiten. Zum Signieren ist der „private" Schlüssel erforderlich, der sich lediglich im Besitz des Unterzeichners befinden darf – zum Beispiel auf einer Chipkarte, die mit einer Geheimzahl (PIN) gesichert ist. Mit dem zugehörigen „öffentlichen" Schlüssel, der allen Kommunikationspartnern bekannt sein kann, läßt sich die Gültigkeit der Signatur und die Unverfälschtheit des signierten Dokumentes prüfen.

Im Signaturgesetz werden die Anforderungen an die **Zertifizierungsstellen** beschrieben, die die Zuordnung eines öffentlichen Schlüssels zu einer Person durch ein Signaturschlüssel-Zertifikat bestätigen und dieses online nachprüfbar oder – mit Zustimmung der Person – abrufbar halten.

Ein Signaturschlüssel-Zertifikat könnte folgendermaßen aussehen:

Name des Signaturschlüssel-Inhabers	Peter Meier
öffentlicher Signaturschlüssel	jöSK9EkQPYTCjkhg8njKAAhl...
Bezeichnung der Algorithmen	RSA
laufende Nummer	4711
Beginn und Ende der Gültigkeit	gültig 01.01.98 – 31.12.2003
Name der Zertifizierungsstelle	Zertify GmbH
Angaben, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art und Umfang beschränkt ist	keine Einschränkung

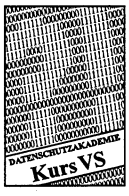
Von den Zertifizierungsstellen dürfen Daten nur erhoben werden, soweit dies zum Zwecke der Ausstellung eines Zertifikates erforderlich ist. Die **Datenerhebung** hat bei den Betroffenen zu erfolgen. Die Verwendung der personenbezogenen Daten zu einem anderen Zweck, z. B. zur Werbung, darf nur mit Einwilligung des Betroffenen erfolgen. Positiv zu bewerten ist auch, daß – ebenso wie bei den Telediensten – die **Datenschutzaufsichtsbehörden** bei den Zertifizierungsstellen auch dann Kontrollen durchführen können, wenn es keine konkrete Anhaltspunkte für einen Datenschutzverstoß gibt.

Im Zertifikat kann statt des Namens auch ein eindeutiges **Pseudonym** angegeben werden, das bei der elektronischen Unterschrift verwendet werden kann. Gerade in Datennetzen lassen sich aus mit dem Namen signierten Daten Persönlichkeitsprofile (z. B. bezüglich des Kaufverhaltens) erstellen, die bei Pseudonymen aber nicht so leicht einer realen Person zugeordnet werden können. Pseudonyme dürfen unter bestimmten Voraussetzungen zur Strafverfolgung oder von den Geheimdiensten aufgedeckt werden. Nach dem Signaturgesetz muß der Nutzer über die Auf-

> ? ***Pseudonym nach dem Signatur gesetz***
>
> *Will man nicht unter seinem richtigen Namen auftreten, z. B. um Datenprofile zur Person zu vermeiden, kann man nach dem Signaturgesetz auch Pseudonyme verwenden. Jedes Pseudonym muß als solches gekennzeichnet und unverwechselbar sein. Die Zuordnung der Pseudonyme zur Person wird bei der Zertifizierungsstelle gespeichert.*

deckung seines Pseudonyms informiert werden, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird.

Der private Schlüssel darf nach dem Signaturgesetz im Gegensatz zum öffentlichen Schlüssel nicht bei der Zertifizierungsstelle gespeichert sein, damit er nicht hinter dem Rücken des Schlüsselinhabers von Unbefugten zum Signieren mißbraucht werden kann. Auch müssen die technischen Komponenten wie z. B. die eingesetzten Chipkarten ein **Auslesen** oder eine **Kompromittierung** des geheimen Schlüssels **verhindern**.



Die Sicherheit und Authentizität der elektronischen Kommunikation ist auch für den Datenschutz ein wichtiges Anliegen. Daher haben wir schon verschiedene Gespräche mit bestehenden und potentiellen **Trustcentern** geführt, um uns über die praktische Umsetzung des Gesetzes zu informieren und auf die datenschutzkonforme Gestaltung des Verfahrens hinzuweisen. Einige Firmen sind von sich aus auf uns zugekommen und haben um Beratung gebeten.

Was ist zu tun?
Bei einer elektronischen Kommunikation in Rechnernetzen sollten sich die Bürger der Möglichkeit der digitalen Signatur immer dann bedienen, wenn sie es zum Schutz ihrer Daten für sinnvoll erachten.

7.3 Verschlüsselung – ein Schlüssel zum Datenschutz

7.3.1 Hände weg von der Kryptographie

In der Fachwelt herrscht zwar Einigkeit darüber, daß ein Verbot der Verschlüsselung weder sinnvoll noch durchsetzbar wäre, doch dies hindert manche Stellen in Bonn nicht daran, weiterhin Pläne für eine Reglementierung zu schmieden.

Die Verschlüsselungsprodukte sind mittlerweile so gut, so weit verfügbar und so leicht einsetzbar, daß jeder seine elektronischen Daten vor unberechtigtem Zugriff schützen kann. Dieses hohe Maß an Vertraulichkeit macht den Sicherheitsbehörden verständliche Sorgen, weil künftig **staatliche Überwachungsmaßnahmen** ins Leere laufen könnten. Schon seit mehreren Jahren prüft die Bundesregierung daher, ob bei Vorliegen einer rechtmäßigen Überwachungsanordnung im Falle einer verschlüsselten Kommunikation eine Entschlüsselung möglich sein muß.

Mögliche Formen einer **Krypto-Reglementierung** wären ein totales Verbot der Verschlüsselung, die Erlaubnis nur für bestimmte Verfahren mit Entschlüsselungsmöglichkeiten, die den Überwachungsbehörden bekannt sind, oder die Zulassung ausschließlich solcher Verfahren, bei denen die geheimen Schlüssel hinterlegt werden müssen und somit im Zugriff der Überwachungsbehörden stehen.

Jede Form der Krypto-Reglementierung ließe sich aber gerade von gewieften Rechtsbrechern leicht **umgehen** (vgl. 19. TB, Tz. 7.6), z. B. durch Vorverschlüsselung der Daten mit einem anderen Verfahren oder durch Verbergen der Nachrichten in anderen Daten (**Steganographie**). Staatlicher Neugier ausgesetzt blieben nur die „normalen" Bürger. Bei einem generellen Verbot der Verschlüsselung würden ihre legitimen Sicherheitsinteressen mißachtet. In diesem Fall hätten auch nichtstaatliche Angreifer „leichte Beute".

Das weiß auch die **Europäische Kommission**, die im Herbst 1997 in einer Mitteilung über die Verwendung digitaler Signaturen und wirksamer Verschlüsselung zur Gewährleistung von Sicherheit und Vertrauen in elektronische Kommunikation die Mitgliedstaaten aufgefordert hat, unverhältnismäßige Beschränkungen zu vermeiden, da dies einen funktionierenden Binnenmarkt und die Wirtschaft der jeweiligen Nation gefährde. Statt dessen wird von ihr gerade die starke Verschlüsselung als Basis für die Entwicklung des Online-Kommerzes und der Informationsgesellschaft in Europa angesehen. Sie legt großen Wert auf eine öffentliche Diskussion ihrer Mitteilung, um einen Konsens zu erreichen.

> **?** ***Steganographie***
>
> *Wörtlich übersetzt: „verdecktes Schreiben" – die Wissenschaft vom Verstecken von Daten. Während es bei Verschlüsselung um die erkennbare Benutzung eines Kryptoverfahrens zur Chiffrierung einer Nachricht geht, bezeichnet die Steganographie den verdeckten Gebrauch eines Verfahrens, mit dessen Hilfe eine Botschaft in einem scheinbaren Klartext, einem Bild, einer Videokonferenz, in Tondateien o. ä. versteckt wird.*

Teile der Bundesregierung vermeiden dagegen den öffentlichen Diskurs. Vor einer Entscheidung zur Krypto-Reglementierung ist eine **Versuchsphase** von etwa zwei Jahren geplant, in der ggf. unter Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf freiwilliger Basis zertifizierte Verschlüsselungsverfahren genutzt werden können, die eine staatliche **Schlüsselhinterlegung (Key-Escrow)** beinhalten. Damit sollen die Infrastruktur für eine solche Schlüsselhinterlegung und die technischen Details getestet werden. Zum einen werden durch den Aufbau einer Infrastruktur Fakten geschaffen, zum anderen wird der positive Begriff diskretiert.

> **?** ***Key-Escrow***
>
> *Key-Escrow bedeutet die Hinterlegung von Kopien aller geheimen Schlüssel bei einer Vertrauensstelle. Wer Zugriff auf diese Schlüssel hat, kann damit verschlüsselte Nachrichten mitlesen.*

Man spielt bei dieser Idee mit dem **Vertrauen der Nutzer**, die ein zertifiziertes Verfahren als besonders sicher ansehen. In Wirklichkeit haben sie letztlich nur die Wahl zwischen einer Software mit garantierter Hintertür für deutsche staatliche Stellen oder einem anderen Verfahren, das möglicherweise ebenfalls Hintertüren beispielsweise für ausländische Geheimdienste aufweist und damit der Wirtschaftsspionage das Tor öffnet. Doch jede Form der Geheimdienste birgt eine Gefahr des Mißbrauchs, z. B. durch Hacker oder professionelle Geheimdienste. Statt dessen wäre es viel sinnvoller, Verschlüsselungsverfahren und ihre Designkriterien offenzulegen, damit sich unabhängige Experten eine Meinung bilden und über die Sicherheit des Verfahrens öffentlich diskutieren können. Nur durch eine solche Transparenz läßt sich das Vertrauen der Nutzer gewinnen, die ihre Daten in der Informationsgesellschaft schützen wollen.

> **?** ***Key-Recovery***
>
> *Bei Key-Recovery werden die Schlüssel nicht hinterlegt, aber sie können im Bedarfsfall hergestellt werden. Dies wirkt sich z. B. aus, wenn Schlüssel verwendet werden, die bei jeder Kommunikationsverbindung automatisch neu generiert und nur einmal verwendet werden. Auch hier ist ein genereller Zugriff auf den Klartext sämtlicher damit verschlüsselte Kommunikation möglich.*

In diesem Zusammenhang zeichnet sich auf dem **internationalen Markt** für Software eine interessante Entwicklung ab. Kürzlich erregte ein bedeutender amerikanischer Anbieter von Internet-Software einige Aufmerksamkeit, als er ankündigte, zukünftig die Interna in der Funktionsweise seiner Programme offenzulegen.

Damit muß die Software nicht lange als „Black Box" hingenommen werden – jeder interessierte Experte kann jede Funktion bis ins Detail nachvollziehen. So wird nachweisbar, ob ein Programm die versprochenen Funktionsmerkmale tatsächlich aufweist oder möglicherweise Abweichungen beinhaltet. Außerdem können **eigene Sicherheitsmodule** integriert werden. Dies ist besonders wichtig, weil aus den USA exportierte Verschlüsselungssoftware nach dem amerikanischen Recht die Möglichkeit für den Zugriff dortiger Sicherheitsbehörden bieten muß. Gerade hier ist z. B. die deutsche Software-Industrie gefordert, selbst Sicherheitsmodule zu entwickeln und zur Vefügung zu stellen.

Die Einhaltung einer einschränkenden Regelung der Kryptographie wäre kaum wirksam zu kontrollieren. Trotz hohen Kontrollaufwandes und erheblicher Rechtsbeeinträchtigungen vieler Bürger wäre eine gezielte Mißachtung des Gesetzes kaum zu unterbinden. Deshalb würde eine Krypto-Reglementierung bereits gegen das im **Grundgesetz** verankerte Verhältnismäßigkeitsprinzip verstoßen. Sie würde gerade den rechtstreuen Bürgerinnen und Bürgern die Ausübung ihres von der Verfassung garantierten Rechts, selbst ihre Privatsphäre gegen fremde Neugier wirksam zu schützen, unmöglich machen.



Aufkleber, der bei uns erhältlich ist.

Was ist zu tun?
Jeder sollte wirksame Verschlüsselungsverfahren einsetzen, wenn er einen unbefugten Zugriff auf seine Daten verhindern möchte. Der Staat sollte Kryptoverfahren nicht behindern, sondern fördern.

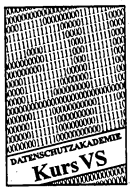
7.3.2 Verschlüsselung von E-Mail an den Datenschutzbeauftragten

Gerade wer den Datenschutz propagiert, muß die Verwendung von Kryptierungsverfahren fördern. Deshalb nehmen wir E-Mails auch gerne verschlüsselt entgegen.

Wer in offenen Netzen wie z. B. dem Internet Informationen austauschen will, kann sich gegen Mitlesen durch unbefugte Dritte nur durch Verschlüsselung der zu übermittelnden Daten wirksam schützen. Dies ist in Deutschland bislang noch in keiner Weise gesetzlich beschränkt. Deshalb empfehlen wir, von Verschlüsselung wirksameren Gebrauch zu machen, wann immer es möglich ist (vgl. Tz. 7.3.1).

> ***? PGP***
>
> *Bei PGP (Pretty Good Privacy) handelt es sich um eine im Internet weit verbreitete Software, mit der man E-Mails verschlüsseln und digital signieren kann. Das Programm, das 1991 vom US-Amerikaner Phil Zimmermann entwickelt wurde, läßt sich auf allen gängigen Betriebssystemen einsetzen. Es basiert auf asymmetrischer Verschlüsselung, d. h. jeder Nutzer besitzt ein Paar aus einem öffentlichen Schlüssel, den er seinen Kommunikationspartnern zur Verfügung stellt, und einem privaten Schlüssel, den er geheimhalten muß, damit nur er die Nachrichten an ihn entschlüsseln kann.*

Da sich Bürger immer häufiger auch per **E-Mail** an unsere Dienststelle wenden, haben wir im Berichtsjahr die Möglichkeit geschaffen, diese auch verschlüsselt zu übermitteln. Dafür wird die Verschlüsselungssoftware **„Pretty Good Privacy" (PGP)** angewandt, die in verschiedenen Versionen kostenlos im Internet bereitsteht. Mit PGP kann auch digitale Signatur realisiert werden. Diese ermöglicht es, eine Nachricht dem Absender sicher zuzuordnen und eine Fälschung oder eine nachträgliche Veränderung von elektronischen Dokumenten für den Empfänger erkennbar zu machen, sofern uns der öffentliche Schlüssel des Absenders bekannt ist.



Unser öffentlicher PGP-Schlüssel, der für die Verschlüsselung von Nachrichten an uns benötigt wird, sowie weitere Informationen über die Verfahrensweise sind sowohl auf unserer Homepage (http://www.schleswig-holstein.datenschutz.de) verfügbar als auch auf Diskette bei uns erhältlich. Wer bereits PGP einsetzt, kann die Echtheit unseres Schlüssels mit dem folgenden „**Fingerprint**", d. h. der Prüfsumme unseres Schlüssels, verifizieren:

042D 0B0E 6D4F F4D3 FB5D 1B6A 318C B401

Was ist zu tun?
Wer mit der Dienststelle des Landesbeauftragten für den Datenschutz elektronisch kommunizieren möchte und verhindern will, daß Dritte mitlesen, sollte seine E-Mail verschlüsseln. Auch andere öffentliche Stellen sollten derartige Möglichkeiten anbieten.

7.4 Problematische neue Abhörbestimmungen

Das Begleitgesetz zum Telekommunikationsgesetz (TKG-Begleitgesetz) enthält neben unproblematischen Anpassungsvorschriften auch einige hochbrisante Regelungen.

Mit dem Telekommunikationsgesetz (TKG) regelt der Bundesgesetzgeber die Rahmenbedingungen der seit Anfang 1998 vollständig liberalisierten Telekommunikation. Es enthält neben Vorschriften zum Datenschutz auch Regelungen dazu, welche Daten die Sicherheitsbehörden von den Betreibern von Telekommunikationsanlagen erhalten können (vgl. 19. TB, Tz. 7.3.1). Im Januar 1998 ist nun das „Begleitgesetz zum Telekommunikationsgesetz" in Kraft getreten. Mit ihm werden eine Vielzahl von bestehenden Gesetzen an das TKG angepaßt.

Problematisch sind aus unserer Sicht folgende Neuregelungen:

7.4.1 Beihilfe zum Abhören

Das Gesetz sieht eine deutliche Ausweitung der Mitwirkungspflichten der Betreiber bei der Überwachung der Telekommunikation vor. Bisher waren nur die Betreiber von Fernmeldeanlagen, die für den **öffentlichen Verkehr** bestimmt sind, verpflichtet, den Sicherheitsbehörden das Abhören der Telekommunikation an diesen Anlagen zu ermöglichen. Nicht davon erfaßt waren solche Dienste, die in **geschlossenen Benutzergruppen** (oder Corporate Networks) nur für eine beschränkte Anzahl von Teilnehmern zur Verfügung standen. Von seiten der Sicherheitsbehörden wurde geltend gemacht, daß kriminelle Organisationen ihre Telekommunikation künftig gerade deshalb in geschlossenen Benutzergruppen abwickeln würden, um der Überwachung der Telekommunikation zu entgehen. Daher sollte die Verpflichtung, den Sicherheitsbehörden das Abhören zu ermöglichen, auch auf diesen Bereich ausgedehnt werden.

Die Regelungen des TKG-Begleitgesetzes schießen aber weit über dieses Ziel hinaus. Verpflichtet, das Abhören zu ermöglichen, sind nunmehr alle Stellen, die Telekommunikationsanlagen jedweder Art Dritten zur Nutzung zur Verfügung stellen. Danach müssen auch sämtliche Betreiber von **Telefonnebenstellenanlagen**, die diese nicht nur für eigene Zwecke benutzen, den Behörden das Abhören in diesen Anlagen ermöglichen. Betroffen davon sind nach dem Wortlaut Firmen oder Behörden, die ihren Mitarbeitern auch private Gespräche auf der firmeneigenen Anlage erlauben, ebenso Krankenhäuser, die den Patienten Telefongeräte ans Krankenbett stellen, oder sogar diejenigen Mitglieder von Wohngemeinschaften, die den gemeinsamen Telefonanschluß auf ihren Namen angemeldet haben und den übrigen Mitgliedern der WG das Telefonieren erlauben. Alle Genannten sind nämlich als geschäftsmäßige Erbringer von Telekommunikationsdiensten anzusehen und haben nach dem Wortlaut der neuen Vorschriften zunächst sicherzustellen, daß das Abhören auf ihren Geräten möglich ist. Der Kreis der Verpflichteten soll dem Vernehmen nach durch eine noch zu erlassende Rechtsverordnung eingeschränkt werden. Diese lag jedoch bei Redaktionsschluß des Tätigkeitsberichtes noch nicht vor.

Die Regelung im TKG-Begleitgesetz bleibt kritikwürdig, weil sie die tatsächlichen Möglichkeiten zum **Abhören** der Telekommunikation für die Sicherheitsbehörden **deutlich ausweitet**. Sie macht das Abhören auch bequemer, weil sie eine große Zahl von Betreibern von Telekommunikationsanlagen verpflichtet, auf eigene Kosten dafür zu sorgen, daß die Überwachung möglich ist. Auch dies ist unter dem Gesichtspunkt der Verhältnismäßigkeit äußerst problematisch. Noch nicht absehbar ist, ob sich daraus sogar neue Mißbrauchsmöglichkeiten für andere Personenkreise ergeben.

Was ist zu tun?
Die Landesregierung sollte sich dafür einsetzen, daß der Kreis der Verpflichteten auf schnellstem Wege per Verordnung eingeschränkt wird.

7.4.2 Späte Erkenntnis des Gesetzgebers

Bisher ist im Strafverfahren nach **§ 12 Fernmeldeanlagengesetz (FAG)** der Zugriff auf Verbindungsdaten für die Strafverfolgungsbehörden möglich. Im Gegensatz zum Abhören der Gesprächsinhalte, das nach § 100 a Strafprozeßordnung (StPO) nur beim Vorliegen bestimmter Straftaten zulässig ist, sieht § 12 FAG für den Zugriff auf Verbindungsdaten gerade keine besonderen Voraussetzungen vor. Da diese Daten genauso vom Grundrecht des Fernmeldegeheimnisses aus Art. 10 Grundgesetz geschützt sind, wie die Inhalte der Telekommunikation selbst, ist die Regelung des § 12 FAG nach unserer Auffassung in ihrer jetzigen Form mit der Verfassung nicht vereinbar.

Im Entwurf der Bundesregierung war vorgesehen, den § 12 FAG durch eine neue Regelung in der **StPO** zu ersetzen, nach der der **Zugriff auf Verbindungsdaten** nur dann möglich sein sollte, wenn es sich um Straftaten von „nicht unerheblicher Bedeutung" oder solche handelte, die „mittels der Endeinrichtungen" begangen werden. Zwar genügte die neu vorgeschlagene Regelung nach unserer Ansicht in vielen Einzelaspekten noch immer nicht den Anforderungen des Grundgesetzes. Sie hätte jedoch immerhin eine Verbesserung des Rechtsschutzes gegenüber der Vorgängervorschrift dargestellt.

? *Verbindungsdaten*

Verbindungsdaten sind die Informationen über die näheren Umstände der Telekommunikation. Dazu gehören die Beteiligung bestimmter Personen, die anrufende und angerufene Nummer, Zeit und Dauer der Verbindung, bei der Mobiltelefonie auch die Funkzelle bzw. der Ort, von dem aus kommuniziert wurde. Auch Daten über erfolglose Verbindungsversuche sind Verbindungsdaten.

Im Gesetzgebungsverfahren wurde sie trotzdem überraschend vom Innenausschuß und vom Rechtsausschuß des Bundestages mit der Begründung abgelehnt, sie berücksichtige nicht ausreichend die **speziellen Zeugnisverweigerungsrechte** der Berufsgruppen, die in strafrechtlichen Verfahren die Aussage als Zeuge verweigern könnten. Das betrifft z. B. Rechtsanwälte, Ärzte und Journalisten, die nicht gezwungen werden dürfen, über ihre Klienten, Patienten bzw. Informanten auszusagen. Damit sollen spezielle Vertrauensverhältnisse geschützt werden.

Diese Bedenken sind von uns seit langem immer wieder geäußert worden. Nachdem sie jedoch erst in einem so späten Stadium des Gesetzgebungsverfahrens ernst genommen wurden, wurde die **Chance verpaßt**, eine sinnvolle Verbesserung des Schutzes von Verbindungsdaten zu verabschieden. Der Bundestag hat nämlich die Fortgeltung des § 12 FAG für zwei weitere Jahre beschlossen. Die Bundesregierung wurde aufgefordert, bis zum April 1998 Vorschläge vorzulegen, wie die Zeugnisverweigerungsrechte mit dem Zugriff auf Verbindungsdaten in Einklang gebracht werden können. Im Ergebnis sieht es also wie folgt aus: Da die beste Lösung, nämlich die Einschränkung des Zugriffs der Sicherheitsbehörden auf Verbindungsdaten und ein gleichzeitiger erhöhter Schutz für besondere Berufsgruppen, nicht erreicht werden konnte, wurde auch die zweitbeste Lösung, nämlich wenigstens die Einschränkung des Zugriffs auf die Verbindungsdaten, nicht realisiert. Statt dessen bleibt die schlechteste Lösung vorerst in Kraft.

Was ist zu tun?
Die Landesregierung sollte darauf hinwirken, daß § 12 FAG möglichst bald durch eine neue Regelung in die StPO ersetzt wird, die dem grundrechtlichen Schutz der Verbindungsdaten gerecht wird und auch die Zeugnisverweigerungsrechte angemessen sichert.

7.4.3 Risiken der Mobiltelefonie: Handys als Peilsender und falsche Basisstationen

Offenbar auf Initiative von Polizeibehörden hatte der Bundesrat in seiner Stellungnahme zum TKG-Begleitgesetz eine Reihe von **Verschärfungen** bei den **Überwachungsbefugnissen** der Telekommunikation gefordert. So sollte in der Strafprozeßordnung zum einen festgeschrieben werden, daß außerhalb der eigentlichen Telefonüberwachung die **Aktivmeldungen der Mobiltelefone** in der Weise hätten ausgewertet werden können, daß sich daraus Bewegungsbilder ihrer Benutzer hätten erstellen lassen. Auf der Grundlage des geltenden Rechts sind derartige Datenerhebungen nur zulässig, wenn ein richterlicher Beschluß zur Überwachung der Telekommunikation vorliegt. Die Bundesregierung ist dem Vorschlag des Bundesrates nicht gefolgt.

> **?** ***Aktivmeldungen von Handys***
>
> *Alle angeschalteten Handys melden sich in gewissen Zeitabständen (im Sekunden- bis Minutenbereich) automatisch bei ihrem Netz, um zu signalisieren, in welcher Funkzelle sie gerade erreichbar sind. Zeichnet man diese Meldungen über einen längeren Zeitraum auf, entsteht ein Bewegungsprofil. Die Meldungen werden nach Auskunft der Betreiber jedoch nicht längere Zeit gespeichert.*

Ein zweiter Vorschlag des Bundesrates ging dahin, in der StPO eine Rechtsgrundlage für den Einsatz des sogenannten **IMSI-Catchers** einzufügen. Eine solche Regelung hätte jedoch erhebliche „Nebenwirkungen". Zumindest werden bei dem Versuch, die netzinterne Rufnummer eines Handy-Benutzers zu ermitteln, Teile des Funknetzes lahmgelegt. Sehr wahrscheinlich ist es auch, daß es dabei zum verstärkten Abhören „bei Gefahr in Verzug" ohne richterliche Genehmigung kommt. Unvermeidlich wäre schließlich, daß auch die Kommunikation Dritter überwacht wird, denn häufig wird sich erst nach einem „Hineinhören" in die einzelnen Gespräche feststellen lassen, welches das zu überwachende ist.

> **?** ***IMSI-Catcher***
>
> *Der IMSI-Catcher ist ein Gerät, durch das eingeschaltete Handys mit Hilfe ihrer International Mobile Subscriber Identification (IMSI), einer international eindeutigen Kennung, identifiziert werden können. Zu diesem Zweck spiegelt der IMSI-Catcher den Handys in seiner Nähe eine Basisstation des Funknetzes vor, bei der sich die Handys im Wirkungsbereich – in freiem Gelände kann das mehr als 1 km sein – anmelden. Die Identität des Kunden kann anhand der IMSI mit Hilfe des Netz-Providers ermittelt werden. In einer erweiterten Version eignet sich der IMSI-Catcher auch zum Abhören der Telefonate, indem er dem Handy signalisiert, die Verschlüsselung auszuschalten und das Gespräch im Klartext über die falsche Basisstation abzuwickeln.*

Noch größer ist aber die Gefahr, wenn ein solcher IMSI-Catcher in die falschen Hände kommt, denn dies bedeutet ein nicht zu unterschätzendes **Risiko für die Vertraulichkeit** der Telekommunikation mit Mobiltelefonen. Gerade bei der Wirtschaftsspionage werden interessierte Kreise erhebliche Mittel aufwenden, um fremde Kommunikation mithören zu können. Daher sollte die Bundesregierung alles unternehmen, um den Einsatz des

Gerätes jedenfalls in Deutschland nachhaltig zu unterbinden.

Was ist zu tun?
Die Landesregierung sollte darauf hinwirken, daß der IMSI-Catcher in Deutschland nicht eingesetzt werden darf und seine Verwendung strafrechtlich verfolgt wird.

7.5 Wenn Behörden ins Internet gehen

7.5.1 Sicherheitskonzept und Firewall

Ein Anschluß an das Internet bringt eine Reihe von Datenschutz- und Datensicherheitsrisiken mit sich. Daher muß die Verwaltung besonders umsichtig sein, wenn sie einen Internet-Zugang realisieren will.

Immer wieder hört man von Hackern im Internet, die unter Ausnutzung von Sicherheitslücken Daten mitlesen, fälschen, modifizieren oder löschen können. Tatsächlich birgt die Anbindung an das **Internet ein objektives Sicherheitsrisiko**, weil dieses System von Haus aus primär offen und nicht sicher ist. Dies müssen die Behörden berücksichtigen, wenn sie sich an das weltweite Datennetz anschließen wollen.

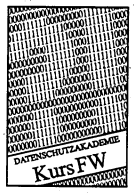
Bei der Planung im Vorfeld muß die Verwaltung zunächst festlegen, welche Daten von wem in das Netz eingespeist und welche Daten von wem abgerufen werden dürfen und darauf ein **Sicherheitskonzept** aufbauen. Darin ist zu bestimmen, auf welche Art und Weise alle nicht gewollten Aktivitäten der eigenen Mitarbeiter oder Außenstehender wirksam verhindert werden können.

Oft reicht es aus, den Zugang zum Internet an einem **abgeschotteten Einzelplatz-PC** zur Verfügung zu stellen, auf dem im übrigen keine schutzwürdigen Daten verarbeitet werden. In diesem Fall wird die Verbindung zum Internet-Provider kontrolliert und nur im Bedarfsfall aufgebaut. Mögliche Schädigungen durch Hacker oder Viren wirken sich dann nur auf den einzelnen PC aus und werden nicht innerhalb der Dienststelle verbreitet.

? ***Firewall***

Eine Firewall („Brandschutzmauer") ist ein System aus Hard- und Software, das ein internes Netz vor unberechtigten Zugriffen aus dem äußeren Netz (z. B. dem Internet) abschottet. Damit läßt sich sicherstellen, daß nur zugelassene netzübergreifende Nutzungen und Zugriffe möglich sind und Mißbrauchsversuche frühzeitig erkannt werden.

Sollte es tatsächlich erforderlich sein, daß viele Mitarbeiter von ihrem Arbeitsplatzrechner im Dienststellennetz aus einen Zugang zum Internet erhalten, muß dieses durch besonders wirksame Maßnahmen abgesichert werden. **Firewalls** („Brandschutzmauern") an der Schnittstelle zwischen lokalem Netz und dem Internet können nur, wenn sie entsprechend professionell gestaltet sind, eine hinreichend hohe Sicherheit gewährleisten. Firewall ist nämlich nicht gleich



Firewall. Es bedarf z. B. umfangreicher Praxistests um festzustellen, ob tatsächlich nur die gewünschten Aktivitäten möglich sind. Bei Organisationsstrukturen mit unterschiedlichem Schutzbedarf sind **gestaffelte Firewall-Lösungen** denkbar, die die Anforderungen der jeweiligen Teilnetze berücksichtigen. Mit der Installation solcher Firewall-Systeme ist es jedoch nicht getan: Die Pflege und Wartung ist in der Regel zeit- und personalaufwendig, um neue Angriffsformen aus dem Internet rechtzeitig erkennen und später bekanntwerdende Sicherheitslücken kurzfristig stopfen zu können.

Was ist zu tun?
Vor dem Zugang zum Internet muß die Verwaltung ein Sicherheitskonzept erstellen, um den Risiken begegnen zu können. Der Aufwand für Pflege und Wartung von Firewall-Systemen darf dabei nicht unterschätzt werden.

7.5.2 Spezielle gesetzliche Rahmenbedingungen

Was viele nicht wissen: Seit kurzem wird die Internet-Benutzung durch das Informations- und Kommunikationsdienstegesetz und den Mediendienste-Staatsvertrag geregelt. Gerade Behörden müssen sich strikt an diese Bestimmungen halten. Die Datenschutzregelungen dieser Gesetzespakete sind von allen Stellen zu beachten, die sich an das Internet anschließen wollen.

Konsequenzen ergeben sich z. B. für diejenigen, die speichern wollen, wie viele Zugriffe auf die eigene Homepage erfolgen. Hierbei stehen verschiedene technische Möglichkeiten zur Verfügung, u. a. ist es auch möglich, die **Internet-Adresse** zu speichern, von der aus der Zugriff erfolgte. Dies ist allerdings nach dem IuKDG und dem MDStV unzulässig.

Problematisch ist auch das Setzen von **Cookies**, wenn sie zur späteren Identifizierung des Benutzers dienen sollen. Die neuen gesetzlichen Regelungen verlangen, daß der Diensteanbieter den Benutzer unterrichtet, wenn ein solcher Cookie gesetzt werden soll. Dies wird bisher allerdings kaum beachtet. Dabei können sich die Diensteanbieter nicht darauf berufen, daß manche **Browser** (wie der Netscape-Navigator) eine Warnung anzeigen. Denn diese Warnhinweis-Funktion ändert nichts an den gesetzlichen Pflichten der Anbieter.

> ***? Browser***
>
> *(von „to browse": engl.: schmökern). Ein Browser ist eine Software, um im Internet auf Angebote im World Wide Web (WWW) zuzugreifen. Damit können – teilweise unterstützt von Hilfsprogrammen – formatierter Text, Graphiken und Videos dargestellt, Formularangaben verschickt oder auch Programme ausgeführt werden, die der Anbieter auf seiner Webseite zur Verfügung stellt.*

Das Erheben und Verarbeiten personenbezogener Daten ist den Diensteanbietern nur zur Durchführung des Dienstes selbst und zu Abrechnungszwecken erlaubt. Sollen darüber hinaus Daten verarbeitet werden, bedarf es selbstverständlich der Einwilligung des Betroffenen. Da in internationalen Rechnernetzen die schriftliche Einwilligung ein eher unbequemes Verfahren darstellt, sehen das IuKDG und der MDStV vor, daß die **Einwilligung** auch **elektronisch** erklärt werden kann. Erforderlich ist dafür allerdings, daß die Einwilligung durch eine eindeutige und bewußte Handlung erfolgt, nicht unerkennbar verändert werden kann und ihr Urheber eindeutig identifizierbar ist. Um diesen Anforderungen zu genügen, muß die Einwilligung mit einer **digitalen Signatur** versehen sein. Es muß sich allerdings nicht um eine Signatur handeln, die von einer zugelassenen Zertifizierungsstelle im Sinne des Signaturgesetzes vergeben wurde. Ausreichend ist es, eine Signatur mit dem Programm PGP zu erzeugen.



? *Cookies*

Cookies sind Variablen, die ein Serverbetreiber auf dem Rechner als Datei abspeichern und später wieder abfragen kann. Ursprünglich sollten Cookies das elektronische Einkaufen erleichtern: Ein Benutzer wählt auf einem Server Waren aus, die er kaufen möchte. Der Server speichert die Kennungen dieser Produkte auf dem Rechner des Nutzers und kann auf der Bestellseite diese Informationen wieder abrufen, um die Bestellung automatisch – bequem für den Käufer – auszufüllen. Ein Server kann Cookies aber auch anbieten, um einen Benutzer beim Betreten der Startseite eindeutig zu markieren und seine Zugriffe auf Folgeseiten von allen anderen Zugriffen unterscheiden zu können. Auf diese Weise ist ein detailliertes Abrufprofil möglich, das sogar einem Namen zugeordnet werden kann, wenn der Benutzer sich im Rahmen einer Bestellung auch nur ein einziges Mal identifiziert.

Was ist zu tun?
Bevor Behörden ins Internet gehen, müssen sie sich mit den neuen Multimediagesetzen auseinandersetzen.

7.6 GeldKarten mit Datenspur

Die GeldKarte soll statt Bargeld als neues Zahlungsmittel zum Einkaufen dienen. Leider wird hierzu keine datenschutzfreundliche Technik verwendet. Die Folge: Wer die Karte benutzt, hinterläßt eine Datenspur.

Ab 1998 können alle Eurocheque-Karten (ec-Karten) auch als elektronische Geldbörse verwendet werden. Immer mehr Händler akzeptieren diese sogenannten GeldKarten, auf deren Chips sich Guthaben von bis zu 400 DM speichern lassen. Beim Aufladen der Karten an speziellen Ladeterminals wird der gewünschte Betrag vom Kundenkonto auf ein gesondertes Börsenverrechnungskonto überwiesen, das die Banken für jeden Kunden eingerichtet haben. Beim Einkaufen kann der Kunde den Betrag von seiner Karte abbuchen lassen, die er zu diesem Zweck mit einer Geheimzahl (PIN) freischalten muß. Der Händler reicht dann die

Zahlungsinformationen an ein Rechenzentrum, die sogenannte **Evidenzzentrale**, weiter, das eine Gutschrift auf seinem Konto veranlaßt und den entsprechenden Betrag vom Börsenverrechnungskonto abbucht.

Die Datensätze, die vom Händler an die Evidenzzentrale weitergeleitet werden, enthalten die Kartennummer, den Kaufbetrag, Kaufdatum, Kaufzeit, einen identifizierbaren Händlerschlüssel und das zum Kaufzeitpunkt aktuelle Kaufsaldo. Zusätzlich zu den Börsenverrechnungskonten der Banken, auf denen nur das Saldo der GeldKarte mitgeführt wird, werden in der Evidenzzentrale kartenbezogene **Schattenkonten** geführt, um eine größere Sicherheit gegen Betrüger und Hacker zu erreichen: Jede Änderung des Kartenguthabens durch Aus- oder Einzahlung wird auf dem Schattenkonto gebucht. Wenn die eingebaute Geldbörse auf der ec-Karte verwendet wird, könnte die Evidenzzentrale zusammen mit der Bank den Personenbezug zu den Buchungen herstellen.

> **?** ***Schattenkonten***
>
> *Schattenkonten dienen dazu, sämtliche Zahlungsvorgänge buchungsmäßig nachzuvollziehen. Alle finanziellen Transaktionen mit einer GeldKarte werden so auf einem kartenbezogenen Schattenkonto, der Börsenumsatzdatei, bei der Evidenzzentrale vermerkt. Zu jedem Zeitpunkt läßt sich darüber das verfügbare Guthaben auf der GeldKarte ermitteln.*

Zwar ist die GeldKarte übertragbar, und es gibt auch „White Cards“ ohne ec-Funktionalität, aus denen weder Name noch Kontonummer des Zahlenden hervorgehen müssen. Doch die **GeldKarte** ist im Gebrauch **nicht so anonym** wie Bargeld und erfüllt damit eine zentrale Anforderung an digitales Geld nicht. Obwohl bei der Auswahl des Kartensystems die Möglichkeit einer tatsächlich anonymen Lösung (vgl. 18. TB, Tz. 7.5) bestanden hätte, hat man sich anders entschieden. Eine anonyme Teilnahme am wirtschaftlichen Leben im gleichen Umfang wie bisher mit Bargeld ist also mit der GeldKarte nicht möglich. Daher wäre es datenschutzrechtlich nicht akzeptabel, wenn man in wichtigen Lebensbereichen zur Benutzung der GeldKarte gezwungen wäre.

Was ist zu tun?
Wer die GeldKarte zum Einkaufen nutzt, sollte sich bewußt werden, daß er eine elektronische Spur hinterläßt.

8. Europa

Rechtzeitige Umsetzung der europäischen Datenschutzrichtlinie in Gefahr

Der Termin zur Umsetzung der EG-Datenschutzrichtlinie rückt näher. Bislang liegt lediglich ein Referentenentwurf für eine Novellierung des BDSG vor. Damit droht die fristgerechte Umsetzung der Richtlinie durch den Bund bis zum Herbst 1998 zu scheitern. Nun sind die Länder gefordert.

Die „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (vgl. 18. TB, Tz. 8.1) gibt **für das Datenschutzrecht einen Mindeststandard** vor, der von allen Mitgliedstaaten der Europäischen Union gewährleistet werden muß. Naturgemäß kommen in europäischen Rechtsnormen die grundlegenden Regelungsgedanken der verschiedenen Rechtsordnungen zum Tragen. Neben deutschen Regelungsmustern finden sich in der Richtlinie vor allem Elemente aus dem französischen Datenschutzrecht. Eine wichtige Grundlage für die EG-Datenschutzrichtlinie stellt auch das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108)" des Europarates vom 18.01.1981 dar. Diese Konvention haben bereits die meisten heutigen Mitgliedstaaten der Europäischen Union unterzeichnet, darunter auch die Bundesrepublik. Griechenland und Italien, die der Konvention des Europarates nicht beigetreten sind, wurden durch die EG-Richtlinie gezwungen, erstmals Datenschutzgesetze zu erlassen.

Die durch die Richtlinie notwendig gewordene Überarbeitung des deutschen Datenschutzrechts birgt die Chance, einige generelle Defizite des in seinen Grundzügen vor 25 Jahren konzipierten Bundesdatenschutzgesetzes, aber auch der Landesdatenschutzgesetze, zu beheben. So lassen sich die **modernen technischen Entwicklungen**, wie z. B. die Datenverarbeitung auf Chipkarten oder die weitgehende Vernetzung der öffentlichen Stellen, mit den bisherigen Ansätzen des Datenschutzrechts nur schwer erfassen. Hinzu kommt, daß viele Bürger einen verbesserten Schutz ihrer Daten gegenüber der privaten Verwertung durch Adreßhandel und Direktmarketing wünschen. Aus unserer Sicht muß das Datenschutzrecht unter folgenden Gesichtspunkten fortentwickelt werden:

- Vergleichbar den Regelungen des IuKDG und des MDStV (vgl. Tz. 7.1) sollte der Grundsatz der **Datensparsamkeit** ebenso festgeschrieben werden wie die möglichst anonyme oder wenigstens pseudonyme Ermöglichung der Inanspruchnahme bestimmter Dienste.
- Überfällig ist die rechtliche Regelung des Einsatzes von **Chipkarten** sowie der **Videotechnik**. Ebenso fehlt es an Vorschriften, die das Problem der **externen Wartung** von Soft- und Hardware regeln, bei der oft personenbezogene Daten den Dienstleistern zur Kenntnis kommen.
- Regelungsbedürftig sind auch **Verbundverfahren**, bei denen verschiedene Stellen mit demselben Datenbestand arbeiten. In diesem Bereich kommt es

erfahrungsgemäß häufig zu einer Verantwortungsdiffusion hinsichtlich der datenschutzrechtlichen Pflichten.

- Besondere Rechtsgefährdungen erwachsen regelmäßig aus Konstellationen, in denen Bürger von anderen Privaten verpflichtet werden, **Selbstauskünfte** einzuholen, die vor Abschluß von z. B. Miet- oder Arbeitsverträgen abzugeben sind. Hier ist ein verstärkter Schutz vor derartigen Verpflichtungen erforderlich.
- Immer wieder klagen die Bürger gegenüber den Datenschutzbeauftragten darüber, daß sie nicht ausreichend gegen **Adreßhandel** und **Direktmarketing** geschützt seien. Insgesamt herrscht ein erhebliches Unbehagen darüber, daß nicht nachvollziehbar ist, wer welche persönlichen Daten über die Betroffenen speichert, verwendet und weitergibt. In diesem Bereich wäre eine Verstärkung der Betroffenenrechte und eine Einschränkung der Zulässigkeit der Datenverarbeitung erforderlich. Wenigstens sollten die Betroffenen auf die Möglichkeit des Widerspruchs gegen die Nutzung ihrer Daten hingewiesen werden müssen. Sinnvoller erscheint jedoch eine Regelung, wonach Werbung und Adreßhandel nur mit ihrer Einwilligung zulässig sind.
- Im Mediendienste-Staatsvertrag findet sich bereits eine Regelung zum **Datenschutz-Audit**, die allgemein in das Bundesdatenschutzgesetz übernommen werden sollte.

Von derartigen neuen Ansätzen findet sich in dem **Referentenentwurf** des Bundesministeriums des Innern zur Novellierung des BDSG allerdings wenig. Der Entwurf betreibt die Umsetzung der Richtlinie vielmehr nach dem Motto „Das Unvermeidliche widerstrebend tun". Dies führt dazu, daß die ohnehin nicht eben leicht verständlichen Regelungen des Datenschutzrechts weiter verkompliziert werden. Die Chance, durch bessere und klarere Regelungen zu einer stärkeren Akzeptanz des Datenschutzes zu kommen, wird damit vertan.

Bei der Formulierung des Entwurfs ist statt dessen mit viel Mühe im Detail versucht worden, die Regelungen der Datenschutzrichtlinie an den verschiedensten Stellen einzeln der aktuellen Fassung des BDSG aufzuoperieren. Das Ergebnis erinnert an einen **Flickenteppich**; das BDSG wird noch schwerer lesbar, als es jetzt schon ist. So hätte, um ein konkretes Beispiel zu nennen, der Begriff der Datenverarbeitung aus der Richtlinie selbst übernommen werden können. Er erfaßt dort sämtliche Phasen der Datenverarbeitung. Eine gleichartige Regelungstechnik findet sich auch im LDSG Schleswig-Holstein. Da allerdings darauf verzichtet wurde, bleibt es bei den mühsamen Aufzählungen, die sich im BDSG bei den einzelnen Zulässigkeitsvoraussetzungen finden, wo jeweils Datenerhebung, -verarbeitung und -nutzung genannt werden müssen.

Weiter hätte es sich angeboten, den Grundsatz der Zweckbindung „vor die Klammer zu ziehen" und im ersten Abschnitt bei den allgemeinen Regelungen einzustellen. Eine derartige Regelung findet sich nicht nur im LDSG Schleswig-Holstein, sondern auch im Gesetzentwurf der Bundestagsfraktion von BÜNDNIS 90/Die GRÜNEN zum Entwurf eines BDSG (BT-Drucksache 13/9082).

Insgesamt ist ein klarer Aufbau des Gesetzes anzustreben; möglichst einfache Formulierungen sollten gewählt werden. Daß dies möglich ist, zeigen die neuen Regelungswerke des Informations- und Kommunikationsdienstegesetzes (IuKDG) und des Mediendienste-Staatsvertrages (MDStV). Die dort enthaltenen Datenschutzvorschriften könnten in dieser Hinsicht als Vorbild dienen.

Wegen der 1998 anstehenden Bundestagswahl muß mittlerweile damit gerechnet werden, daß die **Umsetzung** der Richtlinie **nicht** mehr **zeitgerecht** erfolgen wird. Dies brächte nicht nur Probleme für den Bund mit sich, der mit Ordnungsgeldern der Europäische Union rechnen müßte. Die Länder werden unabhängig vom Bund daran gehen müssen, ihre Landesdatenschutzgesetze an die Richtlinie anzupassen.

Was ist zu tun?
Der Bundesgesetzgeber sollte das BDSG zügig an die EG-Richtlinie und an die technische Entwicklung anpassen. Das Land sollte das LDSG ggf. zeitlich unabhängig davon novellieren.

9. Was es sonst noch zu berichten gibt

9.1 Europäische ISDN-Richtlinie

Die europäische Telekommunikations-Datenschutz-Richtlinie ist nun endlich verabschiedet worden. Sie muß von den Mitgliedstaaten bis zum 24.10.1998 in innerstaatliches Recht umgesetzt werden. Insgesamt ist der Umsetzungsbedarf im deutschen Recht allerdings eher gering (vgl. 19. TB, Tz. 8). Die erforderlichen Anpassungen werden voraussichtlich in einer Rechtsverordnung vorgenommen, die nach § 89 Telekommunikationsgesetz (vgl. 19. TB, Tz. 7.3.1) ergehen wird. Inhaltlich wird sie im wesentlichen auf der bisherigen Telekommunikationsdienst-unternehmen-Datenschutzverordnung (vgl. 19. TB, Tz. 7.3.2) beruhen.

9.2 Wer Forderungen gestundet haben will, muß seine Finanzlage offenlegen – aber wie detailliert?

Zwei Eheleute sollten dem Katasteramt Gebühren für eine Vermessung bezahlen und baten um Stundung. Das Katasteramt verlangte detaillierte Angaben zu ihren Einkommensverhältnissen, um nachprüfen zu können, ob die sofortige Einziehung der Gebühren mit erheblichen Härten für sie verbunden wäre. Um Überprüfung gebeten, ob die erbetenen Auskünfte gegeben werden müßten, kamen wir zu dem Ergebnis, daß dagegen im Prinzip nichts einzuwenden ist. Denn wie sonst sollte über den Stundungsantrag entschieden werden. Da es aber um sensible Angaben ging, halten wir eine Präzisierung der Landeshaushaltsordnung für angezeigt. Denn es kann nicht im freien Ermessen der Verwaltung stehen, wie detailliert Bürger Stundungsanträge begründen und belegen müssen. Das Ministerium für Finanzen und Energie konnte sich diesem Standpunkt bislang noch nicht anschließen.

9.3 Garagenplätze für Frauen scheitern nicht am Datenschutz

Bei einer Kreisverwaltung war die Bauaufsichtsbehörde von der Gleichstellungsbeauftragten um eine Liste der allgemein zugänglichen privaten und öffentlichen Garagen im Kreisgebiet gebeten worden. Das Innenministerium fragte uns, ob dagegen datenschutzrechtliche Bedenken bestünden. Nach dem Gleichstellungsgesetz ist die Gleichstellungsbeauftragte in allen Angelegenheiten des Geschäftsbereiches zu beteiligen, die Auswirkungen auf die Gleichstellung von Frauen haben können. Sie kann in Unterlagen, die zur Erfüllung ihrer Aufgaben erforderlich sind, Einsicht nehmen. Außerdem sind ihr die erforderlichen Auskünfte zu erteilen. Die Neufassung der Garagenverordnung enthält die Verpflichtung, in allgemein zugänglichen Großgaragen mindestens 10 % der Garageneinstellplätze als Frauenparkplätze auszuweisen. Die Voraussetzungen für ein Tätigwerden der Gleichstellungsbeauftragten waren damit erfüllt; folglich bestanden keine Bedenken dagegen, die von der Gleichstellungsbeauftragten gewünschte Auskunft zu erteilen.

9.4 Auftragsvergabe und Frauenquote

Das Ministerium für Frauen, Jugend, Wohnungs- und Städtebau forderte die Landesdienststellen auf, für Zwecke der im Koalitionsvertrag vereinbarten Frauenförderung die Beschäftigtenstrukturen solcher Unternehmen zu analysieren, die Aufträge des Landes erhalten hatten. Neben Art und Umfang der Aufträge sollte die Zahl der beschäftigten Frauen und ihr Anteil an der Zahl der insgesamt Beschäftigten ermittelt, ggf. geschätzt und dem Ministerium mitgeteilt werden. Bei diesen Geschäftsinformationen handelt es sich um personenbezogene Daten, wenn der Unternehmensinhaber eine natürliche Person ist. Leider fehlte für die Sammlung und Weitergabe der gewünschten Informationen eine gesetzliche Grundlage. Die Daten durften also nur mit Einwilligung der Betroffenen zusammengestellt werden. Wir haben vorgeschlagen, künftig im Rahmen der Vertragsgestaltung die Einwilligung für die Verarbeitung der gewünschten Informationen einzuholen.

9.5 Akteneinsicht: Mit gutem Willen auch komplizierte Fälle lösbar

Von dem privaten Träger eines Jugendheimes war ein neuer Erzieher eingestellt worden. Einige Zeit später ging ein Brief bei der Heimaufsicht und dem Ministerium für Frauen, Jugend, Wohnungs- und Städtebau ein, in dem der Absender detaillierte Vorwürfe gegen den Betroffenen erhob. Er begründete sie mit dessen früherer Aufgabe in einer SED-Kreisleitung und im Bildungswesen. Arbeitgeber und Heimaufsicht sahen nach Prüfung trotzdem keine Veranlassung, gegen den Erzieher Maßnahmen einzuleiten. Dieser erhielt Kenntnis von der Existenz des Schreibens und bat unter Hinweis auf das Landesdatenschutzgesetz um Akteneinsicht. Das Ministerium verweigerte sie, weil, selbst wenn die Absenderangabe geschwärzt worden wäre, aus Stil und dargestellten Details des Schreibens ein Rückschluß auf den Absender möglich erschien. Eine unter Umständen nicht unerhebliche Gefährdung seiner schutzwürdigen Interessen wurde befürchtet. Unter unserer Vermittlung gelang es schließlich gemeinsam mit dem Ministerium, den wesentlichen Inhalt des Schreibens in einer Form zugänglich zu machen, die die Offenbarung der Identität des Absenders ausschloß, den Betroffenen aber in die Lage versetzte, die konkreten Vorwürfe zur Kenntnis zu nehmen und sich ggf. dagegen zu wehren.

9.6 Zweckbindung von Daten bei Überweisungen

Kommunale Kassen erhalten regelmäßig im Rahmen des Überweisungsverkehrs Kenntnis von der Bankverbindung ihrer Zahlungspflichtigen. Wir wurden gefragt, ob diese Daten im Falle einer Zwangsvollstreckung auch für eine Kontenpfändung genutzt werden dürfen. Im unbaren Zahlungsverkehr muß der Zahlungspflichtige tatsächlich in Kauf nehmen, daß unabhängig vom eigentlichen Zweck der Zahlung dem Empfänger auch die Bankverbindung bekannt wird und die Kasse auf der Grundlage der Gemeindekassenverordnung befugt ist, in „zweckändernder Weise" zu nutzen. Es bestehen deshalb keine datenschutzrechtlichen Bedenken dagegen,

wenn die im Rahmen des allgemeinen Zahlungsverkehrs bekanntgewordenen Angaben über die Bankverbindung auch für eine Kontenpfändung gegen den Zahlungspflichtigen genutzt werden. Problematischer wird es, wenn die Kasse die Kontoangaben erfragt, um Erstattungen ausführen zu können (vgl. 18. TB, Tz. 4.10.3).

9.7 Übergang der Personalverwaltung auf eine Privatfirma

Trotz der Privatisierung eines kommunalen Eigenbetriebes sollten die dort tätigen Mitarbeiter Beschäftigte der Kommune bleiben und damit weiterhin den Bestimmungen des Landesbeamtengesetzes unterliegen. Dessen Vorschriften beschränken den Zugang zu Personalakten auf „Beschäftigte, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit es zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist". Eine Befugnis zur Übertragung aller Personalverwaltungsaufgaben an private Dritte ist gesetzlich nicht vorgesehen. Sie konnte nur im Einverständnis mit den Betroffenen erfolgen. Im vorliegenden Fall geschah es in Form eines Vertrages, wobei die Anwendung der Schutzvorschriften für den öffentlichen Dienst inklusive der künftigen Änderungen garantiert wurde.

9.8 Retourkutsche auf eine Beschwerde

Ein Bürger, in dessen Nachbarschaft ein Bauvorhaben verwirklicht wurde, hatte sich über das Vorgehen des zuständigen Bauamtes beim Innenministerium als zuständiger Fachaufsichtsbehörde beschwert. Da er Mitarbeiter der Kreisverwaltung war, hatte der für das Bauamt verantwortliche Bürgermeister nichts Eiligeres zu tun, als sich seinerseits bei dem Landrat als Dienstvorgesetztem über den „vorwitzigen" Beschwerdeführer zu beschweren. Es solle geprüft werden, ob der Mitarbeiter dienstliche Hilfsmittel der Kreisverwaltung unbefugt für private Zwecke genutzt habe. Wir hatten aufgrund der Beschwerde des Bürgers zu prüfen, ob die Unterrichtung des Landrates durch den Bürgermeister geltendem Recht entsprach. In seiner Stellungnahme kam der Bürgermeister selbst zu der Erkenntnis, daß die Datenübermittlung nicht zulässig war. Er entschuldigte sich deshalb für den datenschutzrechtlichen Verstoß beim Betroffenen.

9.9 Die Gefängnisverwaltungen dürfen Frauen, die sich vor der Gewalttätigkeit ihrer einsitzenden Lebenspartner fürchten, „vorwarnen"

Im Rahmen eines Beratungsersuchens wurde uns die Frage gestellt, ob gewaltbedrohten Frauen von den Strafvollzugsbehörden Auskünfte über die Unterbringung ihres Lebenspartners insbesondere in der Untersuchungshaft bzw. im Strafvollzug gegeben wurden. Für die betroffenen Frauen ist es von besonderer Wichtigkeit zu erfahren, ob eine Inhaftierung angeordnet war oder eine Entlassung bevorstand, damit sie sich zu ihrem eigenen Schutz darauf einstellen können. Aus datenschutzrechtlicher Sicht gibt es grundsätzlich keine Bedenken, solche Informationen herauszugeben, wenn eine Bedrohungssituation besteht.

9.10 Keine Blankovollmachten bei den Sozialgerichten

Ein Petent hatte beim Sozialgericht Schleswig eine Klage gegen die Bundesversicherungsanstalt für Angestellte eingereicht. Unmittelbar danach wurde er aufgefordert, eine Blankovollmacht zur Befreiung aller relevanten Stellen von Geheimhaltungspflichten bzw. zur Entbindung von der Schweigepflicht zu erteilen. Diese Verfahrensweise war offenbar bei allen Sozialgerichten üblich. Unter Berücksichtigung der richterlichen Unabhängigkeit haben wir angeregt, das Einwilligungsformular künftig nur zu versenden, wenn tatsächlich Daten bei schweigepflichtigen Personen oder Stellen erhoben werden sollten und den Betroffenen genau über den Umfang der einzuholenden Unterlagen zu informieren. Die Sozialgerichte verständigten sich daraufhin landesweit darauf, künftig entsprechend unseren Vorschlägen zu verfahren.

9.11 Akteneinsicht verweigert: Datenschutz gründlich mißverstanden

Ein junger Unternehmer hatte sich selbständig gemacht und ein Existenzgründungsdarlehen bei der dafür zuständigen Bank beantragt. Für diesen Antrag benötigte er auch ein Gutachten über die Erfolgsaussichten seines Betriebes. Das Gutachten wurde von einer Industrie- und Handelskammer erstellt und der Bank übersandt. Als der Darlehenswunsch abgelehnt wurde, bat der Betroffene die Industrie- und Handelskammer um Übersendung bzw. um Einsichtnahme in das Gutachten. Diese lehnte sein Begehren „aus Datenschutzgründen" mit der Begründung ab, daß es sich um einen „vertraulichen hoheitlichen Akt" handele und deshalb die Stellungnahme weder dem Antragsteller noch sonstigen Dritten außer der zuständigen Bank zugänglich gemacht werden dürfe. Der Unternehmer hielt dieses Argument für widersinnig, handelte es sich doch schließlich um ein Gutachten, das er selbst erbeten hatte. Wir konnten seine Auffassung nur bestätigen. Er hatte nach dem Landesdatenschutzgesetz einen Anspruch auf Auskunft bzw. Einsicht in das Gutachten. Das hat schließlich auch die Industrie- und Handelskammer eingesehen und dem Petenten Einblick in das erstellte Gutachten gewährt.

9.12 EIS-Modul nicht gesetzeskonform

Nach den Bestimmungen des Landesmeldegesetzes ist es durchaus gestattet, auch den Mitarbeitern einer Kommunalbehörde, die nicht im Meldeamt tätig sind, einen direkten (online) Zugriff auf die Meldedateien zu geben. Das Gesetz legt für derartige interne Auskünfte ein maximales Datenprofil fest und knüpft alle Auskünfte an die „Erforderlichkeit zur Aufgabenerfüllung". Im Rahmen von Prüfungen haben wir jedoch festgestellt, daß ein geprüftes und freigegebenes Modul des von vielen Kommunen eingesetzten Einwohnerinformationssystems (EIS) der Datenzentrale Differenzierungen nicht vorsieht. Jeder, der das betreffende Programm aktivieren darf, erhält, wenn er will, alle maximal möglichen Daten angezeigt. So könnte man sich zum Beispiel täglich eine Liste über die Bürger

seiner Gemeinde erstellen lassen, die am betreffenden Tag Geburtstag haben. Zur Zeit beraten der Innenminister und die Datenzentrale darüber, wie das Modul zu modifizieren ist.

9.13 Telefongespräche Gefangener

In den Justizvollzugsanstalten werden in Einzelfällen die Telefongespräche der Gefangenen aus Gründen der Sicherheit der Justizvollzugsanstalt überwacht. Dies geschieht zwar mit Wissen der Gefangenen, nicht aber der externen Fernsprechteilnehmer. Zur Begründung wurde vorgetragen, bei Vermittlungen von Telefongesprächen durch JVA-Bedienstete müsse man ohnehin mit einer Überwachung rechnen. Unsere Intervention wurde jedoch zum Anlaß genommen, die Anstalten generell anzuweisen, daß im Falle des Mithörens von Telefongesprächen der auswärtige Gesprächsteilnehmer in Zukunft bei der Vermittlung des Gesprächs ausdrücklich auf die Überwachung hingewiesen wird.

9.14 Wenn der Vollzugsabteilungsleiter mal eben mit dem Hotel telefoniert

Ein Strafgefangener hatte während eines ihm gewährten Hafturlaubes in einem Hotel übernachtet, obwohl er dieses nicht als seine Urlaubsadresse angegeben hatte. Als die Rechnung des Hotels einging, nahm die Vollzugsleitung deshalb einen Verstoß gegen eine vollzugliche Weisung an. Sie setzte sich telefonisch mit dem Hotel in Verbindung und offenbarte die Inhaftierung des Petenten. Dies wurde damit begründet, daß überprüft werden sollte, inwieweit ein Verstoß gegen eine Urlaubsweisung begangen wurde, um die daraus zu folgernden vollzuglichen Konsequenzen zu ziehen. Für uns war nicht nachvollziehbar, welche weiteren Erkenntnisse durch einen Anruf bei dem Hotel erlangt werden sollten, die für eine etwaige Maßregelung des Betroffenen relevant gewesen wären. Die Weitergabe der äußerst sensiblen Information, daß es sich bei dem Betroffenen um einen Strafgefangenen handelte, wurde als ein erheblicher datenschutzrechtlicher Verstoß beanstandet.

10. Rückblick

10.1 Videoüberwachung im Straßenverkehr

Wir hatten in unserem 18. Tätigkeitsbericht (Tz. 4.2.5) kritisiert, daß bei Videoaufzeichnungen im Rahmen der Verkehrsüberwachung nicht nur Verkehrssünder, sondern auch alle gesetzestreuen Autofahrer erfaßt werden. Eine Rechtsgrundlage gibt es hierfür nicht. Die Polizei hatte ihr Verfahren daraufhin dahin gehend modifiziert, daß die bei der Auswertung der Videoaufnahmen festgestellten Verstöße aus dem Überwachungsvideo herauskopiert, auf einem separaten Videoband archiviert und alle nicht benötigten Bildsequenzen vernichtet werden. Darin war zwar eine datenschutzrechtliche Verbesserung zu sehen. Rechtlich zulässig ist es jedoch lediglich, mit Hilfe der Videotechnik von vornherein nur solche Verkehrsteilnehmer zu erfassen, gegen die zumindest ein Anfangsverdacht erkennbar ist. Inzwischen konnte erreicht werden, daß die Polizei eine Technik einsetzt, die es gewährleistet, daß nur noch verdachtsfallbezogene Fahreraufzeichnungen angefertigt werden. Dabei wird der Aufzeichnungsvorgang erst aktiviert, wenn auf dem Überwachungsmonitor ein Verstoß festgestellt wird.

10.2 Neue polizeiliche Vernehmungs- und Anhörungsvordrucke

Im 19. Tätigkeitsbericht (Tz. 10.6) hatten wir dargestellt, daß die von der Polizei im Rahmen der Beschuldigtenvernehmung verwendeten Anhörungsbögen den Umfang des Aussageverweigerungsrechtes inzwischen klar wiedergeben. Dies bezog sich auf den Bereich des Strafverfahrens. Noch ungeklärt war dagegen die Ausgestaltung der Formulare in Angelegenheiten, die lediglich den Vorwurf einer Ordnungswidrigkeit beinhalten. Hierzu hat uns das Innenministerium mitgeteilt, daß derzeit sämtliche Polizeivordrucke mit ähnlicher Rechtsproblematik überarbeitet würden und dabei der Anhörungsbogen für Ordnungswidrigkeitenverfahren vordringlich berücksichtigt werde. Bislang liegt eine Neufassung der Formulare jedoch noch nicht vor.

10.3 Verarbeitung von Versichertendaten im Auftrag (Prüfung IKK)

Bei einer Überprüfungsmaßnahme in einer Krankenkasse im Jahre 1996 war von uns unter anderem beanstandet worden, daß man sich dort eines Rechenzentrums in Nordrhein-Westfalen bediente, ohne die besonderen sozialgesetzlichen Regelungen für die Verarbeitung von Sozialdaten im Auftrag einzuhalten (vgl. 19. TB, Tz. 4.7.6). Mittlerweile liegt eine neue Entwurfsfassung des Vertrages der Krankenversicherung mit dem betreffenden Rechenzentrum vor, der den Anforderungen des Sozialgesetzbuches an eine Auftragsdatenverarbeitung Rechnung trägt. Die allgemeine Klausel, das Rechenzentrum werde bei der auftragsweise durchzuführenden Datenverarbeitung die Bestimmungen für den Datenschutz und für die Datensicherheit berücksichtigen, ist ersetzt worden durch eine detaillierte Regelung, die u. a. auch die technischen und organisatorischen

Maßnahmen zum Datenschutz und zur Datensicherheit im einzelnen festlegt.

10.4 Weitergabe eines Strafurteils entgegen den Bestimmungen des Bundeszentralregistergesetzes

Im 19. Tätigkeitsbericht (Tz. 5.2) hatten wir darüber berichtet, daß ein Petent in einem zivilrechtlichen Gerichtsverfahren mit einem Strafurteil, das vor über 10 Jahren gegen ihn erging, konfrontiert wurde. Die nach den Vorschriften des Bundeszentralregistergesetzes vorgesehene Tilgungsfrist war bereits abgelaufen und die Verurteilung dürfte dem Betroffenen deshalb im Rechtsverkehr nicht mehr vorgehalten oder zu seinem Nachteil verwertet werden. Auf welchem Weg der gegnerische Rechtsanwalt das Strafurteil erhalten hatte, konnte auch durch ein eingeleitetes staatsanwaltschaftlichen Ermittlungsverfahren nicht geklärt werden.

10.5 Nicht nur unzulässige CD-Roms mit Telefondaten

Im 19. Tätigkeitsbericht (Tz. 7.4) hatten wir ausgeführt, daß Telefon-CD-ROMs nur dann zulässig sind, wenn die Betroffenen nach Aufklärung nicht widersprochen haben. Die Telekom hat mittlerweile ihre Kunden angeschrieben und sie auf ihr Widerspruchsrecht hingewiesen. Nach unserer Kenntnis wurden die Widersprüche der Telefonteilnehmer in der aktuellen CD-ROM-Version der Telekom-Tochterfirma DeTeMedien berücksichtigt, so daß Kunden, die dies wünschen, nun gar nicht mehr oder nicht mehr mit Adresse in dem elektronischen Verzeichnis vermerkt sind. Die Nutzung einer solchen CD-ROM als elektronisches Telefonbuch durch Verwaltungsbehörden ist damit datenschutzrechtlich unbedenklich.

10.6 Neue Gaststättenverordnung bringt endlich Klarheit in das Konzessionsverfahren

Über die von uns durchgeführten Prüfungen gaststättenrechtlicher Erlaubnisverfahren haben berichtet (vgl. 17. TB, Tz. 4.3.5 und 18. TB, Tz. 4.1.3). Dabei hatte sich auch die Notwendigkeit gezeigt, die Gaststättenverordnung als Befugnisgrundlage für das Verwaltungsverfahren an die Vorgaben des Landesdatenschutzgesetzes sowie der Gewerbeordnung anzupassen. Unter unserer Mitwirkung wurde nun eine Neufassung der Gaststättenverordnung veröffentlicht, die nicht nur datenschutzrechtlichen Ansprüchen gerecht wird, sondern auch einen Beitrag zur Verschlankung der Verwaltung leistet.

Die neue Gaststättenverordnung schreibt jetzt verbindlich vor, wie im Regelfall ein Erlaubnisverfahren durchzuführen ist, insbesondere welche Angaben bei den Betroffenen zu erheben sind und welche Stellen am Verfahren beteiligt werden dürfen. Durch inhaltlich verbindliche Vordrucke für Antragstellung und Bescheiderteilung konnte auf sprachlich komplizierte Regelungen in der Verordnung weitestgehend verzichtet werden. Die Neuregelung könnte insoweit auch für andere Bereiche vorbildlich sein.

10.7 Krankenscheine für Sozialhilfeempfänger neu gestaltet

Noch immer rechnen einige Kreise Schleswig-Holsteins ärztliche und zahnärztliche Behandlungen von Sozialhilfeempfängern nicht über die Krankenkassen, sondern direkt mit der Kassenärztlichen bzw. Kassenzahnärztlichen Vereinigung ab. Hierfür erhalten die Betroffenen Behandlungsausweise, auf denen neben der Angabe des jeweiligen Sozialhilfeträgers sowie des Aktenzeichens auf der Vorderseite ein großes „S“ zu sehen war. Außerdem waren sie in einem auffälligen Orangeton gehalten. Wer sich auskannte im Sozialhilfebereich wußte gleich Bescheid. Diese äußere Gestaltung empfand eine Bürgerin zu Recht als diskriminierend und wandte sich an uns. Durch Intervention bei den betreffenden Stellen sowie bei dem mit der Herstellung der Vordrucke befaßten Verlag konnte erreicht werden, daß die Krankenscheine nunmehr auf neutralem weißem Papier gedruckt werden.

11. Einige Beispiele, was durch unsere Tätigkeit besser geworden ist

Datenschutzbeauftragte haben die Aufgabe zu kontrollieren und zu kritisieren, wenn sie Mängel bei der Verarbeitung personenbezogener Daten feststellen. Auch dieser Bericht legt an vielen Stellen den Finger in die Wunde und verweist auf Fehlentwicklungen. Der häufige Gebrauch von Wörtern wie „Kritik", „Bedenken", „Beanstandung" könnte zu dem Schluß führen, als sei die Arbeit der Datenschutzbeauftragten vergeblich. Die Wirklichkeit sieht anders aus. In vielen Bereichen haben wir Jahr für Jahr die Veränderung von problematischen Verfahrensweisen erreicht und auf diesem Weg Risiken für das informationelle Selbstbestimmungsrecht an der Wurzel bekämpft. Diese Zusammenstellung zeigt eine Auswahl von Fällen, in denen wir im vergangenen Jahr erfolgreich auf Verbesserungen hingewirkt haben. Über einige der Fälle ist im Vorstehenden detailliert berichtet.

1. *Wer eine Scheidungsurkunde bei einer anderen Stelle vorlegen muß, möchte nicht unbedingt gleich das gesamte Urteil präsentieren. Bislang gaben die Gerichte auf Anfrage das vollständige Urteil heraus, eine Beschränkung auf den Tenor war die Ausnahme. Ab jetzt wird umgekehrt verfahren.*

2. *Wenn Telefongespräche von Gefangenen überwacht werden, wurde bislang nur der Gefangene darauf hingewiesen, nicht der jeweilige Gesprächspartner. Nunmehr werden auch diese darauf aufmerksam gemacht, daß das Gefängnispersonal das Telefongespräch mithört.*

3. *Bislang wurden im Rahmen der Verkehrsüberwachung per Video alle Autofahrer lückenlos erfaßt, auch wenn sie sich verkehrsgerecht verhielten. Jetzt setzt die Polizei eine neue Technik ein, bei der nur die Autofahrer erfaßt werden, die einen Verkehrsverstoß begehen.*

4. *In einem Kreis gab es deutlich sichtbare gelbe Karten an die Mülltonne, wenn sie nicht ordnungsgemäß gefüllt war. Viele Bürger fühlten sich an den Pranger gestellt. Künftig werden die gelben Karten diskret auf der Innenseite angebracht.*

5. *Bislang dokumentierte die Polizei Datenübermittlungen in ihren Kriminalakten solange, bis die gesamte Akte vernichtet wurde. Waren einzelne Informationen schon zuvor zu löschen, konnte man ihren Inhalt gleichwohl noch aus der Dokumentation früherer Übermittlungen ersehen. Nun werden die entsprechenden Informationen bei Fristablauf tatsächlich restlos gelöscht.*

6. *In einigen Kreisen mußten Sozialhilfeempfänger beim Arzt einen auffallend orange gefärbten Krankenschein vorlegen, was viele Betroffene empörte. Künftig werden die Krankenscheine für Sozialhilfeempfänger auf neutralem weißen Papier gedruckt.*

7. Bei der Ahndung von Verkehrsverstößen wurden die „Sünder" bislang nicht über die Datenerhebung und ihre Rechtsgrundlage aufgeklärt. Der entsprechende Vordruck wurde jetzt bundesweit geändert und enthält die notwendige Aufklärung der Betroffenen.

8. Die Datenverarbeitung beim polizeilichen Staatsschutz entsprach in mehrfacher Hinsicht nicht den gesetzlichen Vorschriften. Dadurch drohten gerade in diesem Bereich Beeinträchtigungen wichtiger Grundrechte. Jetzt wurde die Verfahrensweise grundlegend umgestellt.

9. Im Rahmen des Täter-Opfer-Ausgleichs erhalten die beteiligten privaten Träger der Straffälligenhilfe sensible Daten über Täter und Opfer. Künftig müssen sie sich verpflichten, die Regelungen des Datenschutzgesetzes einzuhalten, den Zweckbindungsgrundsatz strikt zu beachten und nach Abschluß des Täter-Opfer-Ausgleichs alle Unterlagen wieder an die Justiz zurückzugeben.

10. Verkehrs-Bußgeldfälle wurden im Computer nach Fristablauf umgehend gelöscht, in den Akten wurden die gleichen Informationen weiter aufbewahrt. Eine neue Aufbewahrungsregelung wird künftig die Frist für die Aktenspeicherung drastisch verkürzen.

11. Ein Sozialamt verlangte von Antragstellern routinemäßig eine pauschale Einwilligung zum Einblick in sämtliche Bankkonten. Künftig werden solche Einwilligungen nur erbeten, wenn im konkreten Einzelfall hierfür eine Notwendigkeit besteht.

12. Bei der Polizei wurden Gehaltspfändungen, auch wenn es sich um minimale Beträge handelte, immer dem Fachvorgesetzten zugeleitet. Durch einen neuen Runderlaß wurde angeordnet, daß der Fachvorgesetzte nur bei Erforderlichkeit unterrichtet werden darf.

13. In einem Sozialgericht wurden Videobilder von Antragstellern aufgenommen und in die Pförtnerei übertragen. Dort konnten auch Dritte mitsehen und mithören. Die Videoanlage wurde abgeschaltet.

14. Wer eine Gaststättenerlaubnis beantragte, mußte bislang damit rechnen, daß bei der Überprüfung seiner Zulässigkeit nicht datenschutzgerecht verfahren wurde. Insbesondere konnten hinter seinem Rücken Erkundigungen eingezogen werden. Jetzt bringt eine neue Gaststättenverordnung erhebliche datenschutzrechtliche Verbesserungen für die Betroffenen.

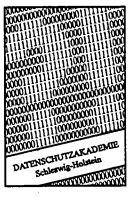
15. Werden „händlerfrische" PC ohne spezielle Veränderungen am Betriebssystem eingesetzt, muß man davon ausgehen, daß sie nur unzureichend gegen unbefugte Benutzungen abgesichert sind. Es besteht dann die Gefahr, daß Personaldaten, sensible Verfahrensdaten und sonstige vertrauliche Unterlagen in die falschen Hände gelangen. Das Innenministerium hat nun

mit der Definition der IKOTECH-Arbeitsplätze einen Sicherheitsstandard geschaffen, der die Risiken von Fehlentwicklungen in den Behörden reduziert.

16. *Wenn die Verantwortungsträger in einer Behörde beim Erwerb von Computerhardware und Programm sich nicht darum kümmern, was anschließend damit geschieht, ist ein Wildwuchs geradezu vorprogrammiert. Welche Daten auf welchen Systemen zu welchen Zwecken wie lange gespeichert werden, kann schon nach kurzer Zeit nicht mehr überblickt werden. Mehr und mehr Verwaltungsleiter haben sich von uns davon überzeugen lassen, daß sie sich die grundsätzlichen Entscheidungen über die Art und Weise des IT-Einsatzes nicht aus der Hand nehmen lassen dürfen; ihre erste „Amtshandlung" bestand dann in der Regel darin, daß überflüssige Datenbestände gelöscht wurden.*

17. *Bei unseren Prüfungen stellen wir vielfältige Sicherheitsmängel fest und machen Vorschläge zu deren Behebung. Fast immer geht es dabei auch um die Wahrung der Vertraulichkeit sensibler Daten gegenüber Dritten. Von Ausnahmen abgesehen, zeigten sich die Behörden einsichtig und sorgten unverzüglich dafür, daß z. B. Diskretionszonen eingerichtet, Unterlagen verschlossen und nicht benutzte PC gegen unbefugten Zugriff gesichert wurden.*

12. DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN



Im vergangenen Jahr hat die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN insgesamt wieder 33 Kurse abgehalten. Seit ihrer Gründung vor fünf Jahren hat die DATENSCHUTZAKADEMIE damit 93 Kurse mit ca. 2.500 Teilnehmern aus Schleswig-Holstein und dem ganzen Bundesgebiet durchgeführt. Die Nachfrage nach den Veranstaltungen der DATENSCHUTZAKADEMIE hat auch im Berichtsjahr unvermindert angehalten.

Das Jahresprogramm 1998 trägt den neuen Entwicklungen im Datenschutzrecht Rechnung. Die Multimediagesetze, das Signaturgesetz, Internet und Verschlüsselung sind Themen, die erstmals in eigenen Kursen behandelt werden.

Da die Bürgerinnen und Bürger ihre datenschutzrechtlichen Belange in einigen Bereichen selbst in die Hand nehmen können, wendet sich das neue Jahresprogramm erstmals nicht nur an Behörden- oder Firmenmitarbeiter. Jeder der erfahren möchte, wie er seine Privatsphäre z. B. durch Verschlüsselung oder digitale Signatur selbst schützen kann, kann an den entsprechenden Kursen teilnehmen.

Das Jahresprogramm '98 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

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
Kurse/Seminare/Workshops 1998

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
Datenschutz an der Schule	L 14	12.03.1998	Kiel
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 4	19.03.1998	Bordesholm
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	SI 4	23.03.-25.03.1998	Leck
Schutz von Personaldaten	P 6	21.04.-22.04.1998	Bordesholm
Datenschutz in Netzen	EN 2	23.04.1998	Kiel
Datenschutz an der Schule	L 15	30.04.1998	Kiel
Verschlüsselung und digitale Signatur	VS 1	05.05.1998	Kiel
Einführungskurs Kommunalbereich	EK 3	07.05.1998	Kiel
Behördliche Datenschutzbeauftragte	D 8	11.05.-15.05.1998	Leck
Einstieg in das Datenschutzrecht	E 4	05.06.1998	Kiel
Führung von Personalakten	PA 5	09.06.-10.06.1998	Bordesholm
Internet für Behörden	INT 1	30.06.1998	Kiel
Datenschutz für den Medizinischen Dienst	MD 1	07.09.-11.09.1998	Leck
Kommunalbereich	EK 4	10.09.1998	Kiel
Einstieg in das Datenschutzrecht	E 5	17.09.1998	Kiel
Datenschutz an der Schule	L 16	24.09.1998	Kiel
Technik und Recht von Firewalls	FW 1	29.09.1998	Kiel
Datenschutz an der Schule	L 17	01.10.1998	Kiel
Multimedia – Rechte der Nutzer/Pflichten der Anbieter	MM 1	06.10.1998	Kiel
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 5	08.10.1998	Bordesholm
Workshop zur Datensicherheit	SIW 3	29.10.-30.10.1998	Leck
Beauftragte für Sozialdatenschutz	S 6	02.11.-06.11.1998	Leck

13. Sommerakademie 1998

SOMMER akademie'98

Die Sommerakademie 1998 findet am

17. August 1998

im Landeshaus in Kiel statt. Derzeit ist folgender Arbeitstitel vorgesehen:

„Der neue Datenschutz"

(„Datenschutz in der Informationsgesellschaft von morgen")

Die Sommerakademie befaßt sich mit neuen Ideen und Ansätzen für die Datenschutzkontrolle. Unter anderem sind Beiträge zu folgenden Themen vorgesehen:

Datenschutzberatung – Hilfe zum Selbstschutz; Online-Kontrollen von der Dienststelle aus; Praxisorientierte Technikfolgenabschätzung; Kooperation der Datenschutzbeauftragten mit Hard- und Softwareentwicklern; Welche technische Ausstattung brauchen die Datenschutzbeauftragten?; Datenschutzkontrollen über die Grenzen hinweg, Auditing durch Datenschutzbeauftragte; Datenschutzbeauftragte als Trusted Third Parties; Neue Kontrollstrategien: Datenschutzbeauftragte als „Tiger-teams"; Personalaustausch und andere flexible Kooperationsformen zwischen den Datenschutzbeauftragten; Aufsicht oder Attacke? Beiziehung externer Spezialisten zu Kontrollmaßnahmen; Datenschutz als Innovationsmotor statt als Technikfeind; Welches Personal brauchen die Datenschutzbeauftragten morgen?; Datenschutzbeauftragte und Informationszugangsrechte; Schutz von Bürgerrechten durch gesellschaftliche Gruppen – die Rolle der Datenschutzbeauftragten; Mitgestaltung von ISO- und DIN-Normen; Plädoyer für einen neuen Ansatz im Datenschutzrecht; Organisation der Datenschutzkontrollstellen in der Zukunft; Professionelle Werbung für ein Grundrecht? Neue Formen der Selbstdarstellung der Datenschutzbeauftragten; Effektive Wahrnehmung des Selbstbestimmungsrechts; Auf den Verwendungszusammenhang kommt es an; Synchronisation der Arbeit der Datenschutzbeauftragten und der Aufsichtsbehörden; Datenschutz – Ein Bürgerservice in der modernisierten Verwaltung; Erwartungen eines betrieblichen Datenschutzbeauftragten an staatliche Datenschutzbeauftragte; Die Rolle der Datenschutzbeauftragten bei der Aushandlung von mehrseitiger Sicherheit; Neue Anforderungen an die Datenschutzkontrolle nach den Multimediagesetzen; Wird es im Jahre 2008 noch Datenschutz geben?

Die **Sommerakademie 1998** soll ein offenes Diskussionsforum zwischen Juristen, Informatikern, Herstellern, Anbietern, Nutzern, Bürgerinnen und Bürgern und Datenschützern sein. An der Vorbereitung und Durchführung der Sommerakademie 1998 wirken u. a. mit:

Landtagspräsident Heinz-Werner **Arens**; Dr. Bruno **Baeriswyl**, Zürich; Dr. Johann **Bizer**; Dr. John **Borking**, The Hague; ehemaliger Innenminister des Landes Schleswig-Holstein Prof. Dr. Hans Peter **Bull**; Prof. Dr. Alfred **Büllesbach;** Dipl.-Inform. Hannes **Federrath**; Dipl.-Inform. Dirk **Fox**; Hansjürgen **Garstka**; Prof. Dr. Rainer **Hamm**; Prof. Dr. P. **Heinzmann**, Rapperswill; ehemaliger Senator der Justizbehörde der Freien und Hansestadt Hamburg Prof. Dr. Wolfgang **Hoffmann-Riem**; Kei **Ishii**, Berlin; Dr. Joachim **Jacob**; Dr. Werner **Kessel**; Thomas **Königshofen**; Ulrich **Kühn**, Prof. Dr. jur. Bernd **Lutterbeck**; Prof. Dr. Albert **von Mutius**; Roland **Müller**; Prof. Dr. Andreas **Pfitzmann**; Kai **Rannenberg**; Prof. Dr. Helmut **Reimer**; Prof. Dr. Alexander **Roßnagel**; Peter **Schaar**, Claus **Schönleber**; Dr. Hans-Hermann **Schrader**; Bettina **Sokol**; Dr. Stefan **Walz**; Dr. Thilo **Weichert**; Dr. Helmut **Bäumler.**

INFORMATION UND ANMELDUNG BEIM

Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1200, Telefax 0431/988-1223
E-Mail: LDSH@netzservice.de

Der Landesbeauftragte für den Datenschutz bei dem Präsidenten des Schleswig-Holsteinischen Landtages

Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1200, Telefax: 0431/988-1223
E-Mail: LDSH@netzservice.de
Internet: www.schleswig-holstein.datenschutz.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:	**Dr. Thilo Weichert** App. 1205

Referat LD 1
Dr. Helmut Bäumler
App. 1200

Silke Molt App. 1203	Vorbereitung der Sitzungen 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 Herausgabe elektronischer Publikationen Betreuung der Homepage im Internet Zusammenstellung und Gestaltung von Seminarunterlagen für die DATENSCHUTZAKADEMIE
Heike Reimann App. 1209 Katrin Caspari App. 1210	Sekretariat Registratur

Referat LD 11	
Lukas Gundermann App. 1215	Grundsatzfragen des Datenschutzes Recht der Neuen Medien Novellierung des Landesdatenschutzgesetzes Automationsvorhaben der Justiz: MEGA, MESTA, automatisiertes Grundbuch
Referat LD 2	
Dr. Thilo Weichert App. 1205	
Jürgen von der Ohe App. 1206	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Ausländer-, Kommunal-, Gewerbe-, Bau- und Wirtschaftswesens Datenschutz im Bereich der Parlamentsverwaltung
Holger Brocks App. 1207	Datenschutz im Bereich der Landwirtschaftsverwaltung, des Kataster-, 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	Datenschutz im Bereich der Steuerverwaltung sowie innerhalb der Dienststelle des Landesbeauftragten für den Datenschutz
Heiko Behrendt App. 1212	Grundsatzfragen der Datensicherung und der ordnungsgemäßen Anwendung der DV-Programme (§§ 7, 8 LDSG) Prüfung von Rechenzentren
Thomas Lenz App. 1219	Prüfung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind
Gebhard Uehlken App. 1229	Mitwirkung bei der Erstellung von Gutachten

Referat LD 4	
Gabriele Lipka	Datenschutz im Sozial- und medizinischen Bereich
App. 1253	
Gabriele Meyer-Bettyn	
App. 1216	
Referat LD 5	
Dr. Susanne Rublack	Datenschutz im Polizei-, Verfassungsschutz- und
App. 1204	Justizbereich
	Internationales Datenschutzrecht
Hans-Jürgen Strasdat	
App. 1217	
Silke Molt	
App. 1203	
Referat LD 6	
Marit Köhntopp	Neue Medien und Informationstechnologien
App. 1214	Kryptographie
	Technikfolgenabschätzung
Jan Ziegler	EDV-Einsatz der Dienststelle
App. 1213	Anbindung der Dienststelle an das Internet und an andere Netze
Frank Möller	Führung und Veröffentlichung der Dateienübersicht
App. 1228	(§ 24 LDSG)

Beim **Landesbeauftragten für den Datenschutz** erhältliche Publikationen

Datenschutz in Schleswig-Holstein (13. Auflage)
Text des Landesdatenschutzgesetzes, der Datenschutzverordnung 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

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Tätigkeitsberichte
der letzten Jahre als Sammlung

Diverse Aufkleber

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 1998
- Dokumentation der Sommerakademie 1997

Datenschutz auf Diskette
Der Landesbeauftragte für den Datenschutz hat eine Diskette herausgebracht, auf der die letzten sechs Tätigkeitsberichte, die Texte des Bundes- und Landesdatenschutzgesetzes und der Datenschutzverordnung, das Programm der DATENSCHUTZAKADEMIE, weitere Publikationen sowie der öffentliche Schlüssel zur vertraulichen E-Mail-Kommunikation gespeichert sind. Die Diskette kann beim Landesbeauftragten kostenlos angefordert werden. Das Programm ist benutzungsfreundlich gestaltet und leicht zu bedienen. Es erlaubt z. B. 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, Windows für Workgroups bzw. Windows 95/NT erforderlich.

Schleswig-holsteinische Datenschutzinformationen im Internet
Auch der Landesbeauftragte für den Datenschutz nutzt moderne Kommunikationstechnologien, um Informationen zu präsentieren. Datenschutzinformationen aus Schleswig-Holstein sind im weltweiten Datennetz Internet zugänglich: **http://www.schleswig-holstein.datenschutz.de** (Homepage des Landesbeauftragten für den Datenschutz Schleswig-Holstein). In der kürzlich auch graphisch überarbeiteten Version sind zur Zeit das Bundes- und Landesdatenschutzgesetz und die Datenschutzverordnung, das Programm der DATENSCHUTZAKADEMIE, die Tätigkeitsberichte der letzten Jahre, Pressemitteilungen und weitere Publikationen im elektronischen Format abrufbar. Weiterhin ist dort der öffentliche Schlüssel für vertrauliche E-Mail-Kommunikation mit dem Landesbeauftragten für den Datenschutz erhältlich.