SCHLESWIG-HOLSTEINISCHER LANDTAG
14. Wahlperiode

Drucksache 14/2080
20. 04. 99

Bericht

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

**Einundzwanzigster Tätigkeitsbericht
(Berichtszeitraum: 1998, Redaktionsschluß: 15.03.1999)**

SCHLESWIG-HOLSTEINISCHER LANDTAG
14. Wahlperiode

Drucksache 14/2080
20. 04. 99

Bericht

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

**Einundzwanzigster Tätigkeitsbericht
(Berichtszeitraum: 1998, Redaktionsschluß: 15.03.1999)**

In der Anlage übersende ich gemäß § 23 Abs. 3 Satz 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen vom 30. Oktober 1991 den einundzwanzigsten 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, Tel. (0431) 6 60 64-0, Fax (0431) 6 60 64-24 zu beziehen.

Inhaltsverzeichnis **Seite**

1.	**Situation des Datenschutzes in Schleswig-Holstein**	**6**
1.1	Bestandsaufnahme	6
1.2	Konsequenzen für ein neues Datenschutzrecht	9
1.3	Die Arbeit der Dienststelle	11
2.	**Der Weg in die Informationsgesellschaft**	**14**
2.1	Fernmeldegeheimnis und Telekommunikation	14
2.2	Frist für die Umsetzung der Europäischen Datenschutzrichtlinie verpaßt	16
3.	**Datenschutz im Landtag**	**18**
3.1	Endlich eine Datenschutzordnung für den Landtag	18
3.2	Behindert Datenschutz die Information der Abgeordneten?	18
3.3	Aufbau des Informations- und Kommunikationssystems	19
4.	**Datenschutz in der Verwaltung**	**21**
4.1	Kommunalbereich	21
4.1.1	Überblick	21
4.1.2	Licht und Schatten bei der Datensicherheit im kommunalen Bereich	21
4.1.3	Prüfung der Versorgungsausgleichskasse	25
4.1.4	Verwaltungsvorschriften zur Aufstellung von Bauleitplänen verbessert	27
4.2	Polizeibereich	28
4.2.1	Überblick	28
4.2.2	INPOL-neu	29
4.2.3	Landespolizeirecht oder Bundeskriminalamtgesetz	30
4.2.4	Genetischer Fingerabdruck	31
4.2.5	Schleierfahndung oder nicht?	33
4.2.6	Prüfungen bei Polizeistationen	34
4.2.7	ZEVIS-Abfrage mit schwerwiegenden Folgen?	35
4.2.8	Evaluierung polizeilicher Befugnisse – Verwaltungsfachhochschule Altenholz startet ein Untersuchungsprojekt	36
4.2.9	Polizeifunk für alle?	37
4.3	Verfassungsschutz – Sicherheitsüberprüfungsgesetz läßt weiter auf sich warten	39
4.4	Justizverwaltung	41
4.4.1	Überblick	41
4.4.2	Datenschutzregelungen für den Strafvollzug	41
4.4.3	Zentrale Register der Staatsanwaltschaften	42
4.4.4	Fehler im Schuldnerverzeichnis	43
4.5	Ausländerüberwachung – ein gesellschaftliches Pilotprojekt?	45
4.5.1	Überblick	45
4.5.2	Asylcard – zwischen Verwaltungseffizienz und Totalkontrolle	46

4.5.3	EURODAC	47
4.5.4	Datenabgleich im Asylbewerberleistungsgesetz	48
4.5.5	Verwaltungsvorschriften zum Ausländergesetz	49
4.6	Wirtschaft, Technik, Verkehr	50
4.6.1	Ausführungsgesetz zur Insolvenzordnung	50
4.6.2	Notwendige Kammermitteilung oder öffentlicher Pranger?	50
4.6.3	Alle Autobahngegner auf einen Blick	51
4.6.4	„Videokameras" an Autobahnbrücken?	52
4.6.5	Zulassungsstellen sind keine Dienstleister für Versicherungen	52
4.7	Sozialbereich	53
4.7.1	Überblick	53
4.7.2	Zum Stellenwert des Sozialgeheimnisses in der AOK Schleswig-Holstein	54
4.7.3	Sozialbehörden künftig Außenstellen der Polizei?	58
4.7.4	Wenn das Sozialamt die Kontoauszüge sehen will	59
4.7.5	Vermieterbescheinigungen für Wohngeldanträge	60
4.7.6	Problematische Datenflüsse	61
4.8	Schutz des Patientengeheimnisses	64
4.8.1	Gesetzgebungsvorhaben	64
4.8.2	Neufassung der Ärztlichen Berufsordnung	64
4.8.3	Patientenakten für die Kassenzahnärztliche Vereinigung?	65
4.9	Schule, Hochschule, Wissenschaft	67
4.9.1	Datenschutzverordnung als „Blockwartsystem"?	67
4.9.2	Schulabgängeradressen für Werbezwecke gesucht!	68
4.9.3	Studi-Chipkarten	69
4.9.4	Was brächte ein Forschungsgeheimnis?	70
4.10	Steuerverwaltung	71
4.10.1	Steuerdatenabrufverordnung – es grenzt an einen Schildbürgerstreich	71
4.10.2	Registrierung von Barzahlern als Druckmittel	72
4.10.3	Restrisiken beim Fax-Verkehr	73
4.10.4	Wahrung des Steuergeheimnisses – in erster Linie eine Frage der Haushaltsmittel?	74
4.11	Personalwesen	75
4.11.1	Modernes Personalmanagement datenschutzgerecht gestalten	75
4.11.2	Der Blick des behördlichen Datenschutzbeauftragten in die Personalakte	78
4.11.3	Verfahren zur Unterrichtung unterlegener Bewerber	79
4.11.4	Versendung von amtsärztlichen Gutachten auf dem Dienstweg	80
4.12	Angekündigte Unangekündigte Kontrollen (AUK)	81

5.	**Datenschutz bei Gerichten**	**84**
5.1	Elektronisches Grundbuch	84
5.2	Nichtöffentliche Verhandlungen vor Finanzgerichten – Theorie und Praxis	87
6.	**Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung**	**89**
6.1	Das „Jahr-2000-Problem" – und was das mit dem Datenschutz zu tun hat	89
6.2	Paßwortsicherheit – ein unterschätztes Problem	90
6.3	Warum gibt es keine Verwaltungsinformatiker?	92
6.4	Innenministerium läßt sich bezüglich der Gestaltung seiner IT-Services beraten	94
6.5	Noch keine konkreten Fortschritte beim Schleswig-Holstein-Netz der Datenzentrale	95
6.6	Datensicherheit à la EU – wenn es ums Geld geht II	95
6.7	Kontrollen im Bereich der automatisierten Datenverarbeitung	97
6.7.1	Hier ist ein Computer – nun nutzt ihn mal schön!	97
6.7.2	Wer trägt die Verantwortung für den Computereinsatz in den Finanzämtern?	99
6.7.3	Computer im Krankenhaus – keiner weiß, wo es lang geht	101
7.	**Neue Medien und Informationstechniken**	**104**
7.1	Internet	104
7.1.1	Anonymer Internet-Zugang	104
7.1.2	Möglichst sicher durch das Internet	105
7.1.3	Gut, daß wir verschlüsselt haben !	109
7.1.4	Platform for Privacy Preferences (P3P): US-Firmen zieren sich	110
7.1.5	Jugendschutz im Internet – Möglichkeiten und Grenzen	112
7.2	Biometrie datenschutzgerecht gestalten	114
7.3	Data-Warehouse und Data-Mining heben Zweckbindung auf	116
7.4	Krypto aktuell	118
7.5	Auf dem Weg zum praktischen Einsatz der digitalen Signatur	120
7.6	Erstmalig Datenschutzanforderungen in den Common Criteria	121
7.7	Umfangreiche Abhörbestimmungen in Vorbereitung	122
7.8	Von der Europäischen Union zur Europäischen Überwachungsunion?	124
7.9	Set-Top-Boxen datenschutzgerecht gestalten!	125
8.	**Europa**	**127**
	EU-Richtlinie zur elektronischen Signatur	127
9.	**Was es sonst noch zu berichten gibt**	**129**
9.1	Polizei bereinigt zügig ihre Personalakten	129
9.2	Neue Datenschutzregelungen im Straßenverkehrsgesetz	129
9.3	Einblick in Gutachten des Medizinischen Dienstes	129
9.4	Zwangsvollstreckung in der Wohngemeinschaft	130
9.5	Neufassung von MiStra und MiZi	130
9.6	Datenzentrale als Privatunternehmen?	130

9.7	Klatsch über Hausdurchsuchung in einer Gemeinde	131
10.	**Rückblick**	**132**
10.1	Terminsaushänge bei nichtöffentlichen Gerichtsverfahren	132
10.2	Nachkontrolle in einer Führerscheinstelle	132
10.3	Datensicherheit bei der Justiz	132
10.4	Neuer Erlaß regelt die Aufbewahrungsfristen von Bußgeldakten	133
10.5	Fahrtenbücher von Ärzten und Apothekern	133
10.6	KomFIT – ein neuer Name, ein neues Konzept	133
10.7	Staatskanzlei startet Pilotprojekt für Telearbeit	133
10.8	Landesinitiative Informationsgesellschaft	134
11.	**Einige Beispiele dafür, was die Bürger von unserer Tätigkeit haben**	**135**
12.	**DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN**	**139**
13.	**Sommerakademie 1999**	**141**
	Anhang	**145**
	Die Vorschläge zur Novellierung des Landesdatenschutzgesetzes auf einen Blick	145
	Vorschlag des Landesbeauftragten für den Datenschutz zur Novellierung des Landesdatenschutzgesetzes	154

1. Situation des Datenschutzes in Schleswig-Holstein

1.1 Bestandsaufnahme

Wenn man die Frage stellt, wie es 1998 um den Datenschutz bestellt war, müssen drei Aspekte unterschieden werden: Die Rechtsentwicklung, die Informationstechnik und die Arbeit in unserer Dienststelle (Tz. 1.3). Würde man einen dieser Bereiche ausblenden, entstünde ein schiefes Bild.

- **Die Rechtsentwicklung**

Die Gesetzgebung war auch im vergangenen Jahr eher durch den Abbau des vom Bundesverfassungsgericht entwickelten Grundrechts auf informationelle Selbstbestimmung als durch seine verbesserte rechtliche Ausgestaltung gekennzeichnet. Die Entstehungsgeschichte, Argumentationen während der Beratungen und die künstliche Hektik bei der Verabschiedung der meisten bereichsspezifischen Vorschriften konnten den Eindruck vermitteln, als müßten vornehmlich und dringendst lästige Hindernisse für die Exekutive beseitigt werden.

Ein typisches Beispiel dafür ist die Aushöhlung von § 68 **Sozialgesetzbuch X**, die mit einem Schlag alle Sozialleistungsträger zu Hilfsorganen der polizeilichen Fahndung gemacht hat. Die Polizei kann jetzt Fahndungslisten, pardon: einzelne Fahndungsfälle, aber insgesamt so viele sie möchte, bei den Sozialbehörden hinterlegen und verlangen, daß sie angerufen wird, wenn die Gesuchten auftauchen oder auch nur ihr Kommen ankündigen. Ein einzelner, in die Presse lancierter Fall in einer süddeutschen Großstadt wurde aufgebauscht und zum Anlaß genommen, den Sozialdatenschutz insgesamt substantiell zu schwächen. Kaum jemand fand sich in der politischen Debatte bereit, das noch vor wenigen Jahren als Errungenschaft gefeierte Sozialgeheimnis zu verteidigen (vgl. Tz. 4.7.3).

Die gesetzliche Grundlage für **Große Lauschangriffe** in Privatwohnungen wurde im Sommer 1998 verabschiedet, ohne daß ein Mindestschutz für die Intimsphäre gewährt wurde. Zwar konnten die massiven Proteste der Berufsverbände und der Datenschutzbeauftragten („Bonner Appell") wenigstens erreichen, daß Ärzte, Journalisten, Rechtsanwälte und andere, die einem besonderen Berufsgeheimnis und Zeugnisverweigerungsrecht unterliegen, nicht abgehört werden dürfen, aber die fundamentale Entwertung des Schutzes der eigenen vier Wände konnte nicht verhindert werden. In der Debatte machte sich außer den Datenschützern kaum jemand für die Privatsphäre der Familien stark (vgl. Tz. 4.2.1).

Das von der Bundesregierung proklamierte Ziel, es dürfe **keine „abhörfreien Zonen"** geben, wurde weiterhin unnachgiebig verfolgt. Das Begleitgesetz zum Telekommunikationsgesetz verpflichtet alle „geschäftsmäßigen Erbringer von Telekommunikationsdiensten" zur Mitwirkung an Abhöraktionen. Der Entwurf der zugehörigen Telekommunikationsüberwachungs-Verordnung, der die Folgen dieser Gesetzgebung plastisch vor Augen führte, mußte wegen des Protestes der Betreiber von Telefonnetzen zunächst zurückgestellt werden; das Vorhaben ist

aber noch nicht vom Tisch. Der ursprüngliche Plan, nämlich auch Krankenhäuser, Hotels, Wohngemeinschaften und Studentenwohnheime zu verpflichten, teure Abhörschnittstellen für Geheimdienste und Polizei bereitzuhalten, falls einmal ein Patient, Gast oder Mitbewohner abgehört werden muß, hat für erhebliche Unruhe gesorgt. Die neue Bundesregierung hat noch nicht verbindlich erklärt, welche dieser Absichten sie zu verwirklichen gedenkt (vgl. Tz. 7.7). Parallel dazu wurde statt dessen von deutscher Seite auf eine Europäisierung der Überwachungsmöglichkeiten gedrängt (vgl. Tz. 7.8).

Ungewöhnliche Eile wurde an den Tag gelegt, als es darum ging, Rechtsgrundlagen für den Aufbau einer Datei mit **genetischen Fingerabdrücken** zu schaffen. In diesem Fall diente ein empörendes Sexualverbrechen als Treibsatz, gegen dessen Dynamik kaum anzudiskutieren war. Auch wenn gegen die Nutzung genetischer Fingerabdrücke für Zwecke der Prävention und der Strafverfolgung grundsätzlich nichts einzuwenden ist, stand die Debatte über die in diesem Zusammenhang zu lösenden hochsensiblen Rechtsfragen von Anfang an unter dem Diktat einer nicht nachvollziehbaren Dringlichkeit. Da das Bundeskriminalamt durch Einrichtung einer Gen-Datenbank vollendete Tatsachen geschaffen hatte, bevor der Gesetzgeber um Erlaubnis dazu gefragt worden war, konnten im Gesetzgebungsverfahren keine gravierenden Änderungen mehr durchgesetzt werden. Die in der Wissenschaft diskutierte Variante, die Durchführung der genetischen Analysen und die Speicherung der Ergebnisse bei einem wissenschaftlichen Institut vornehmen zu lassen, war beispielsweise mit der Einrichtung der Datenbank beim Bundeskriminalamt vom Tisch (vgl. Tz. 4.2.4).

Die seit Jahren überfälligen Datenverarbeitungsbestimmungen für den **Strafvollzug** wurden zwar endlich verabschiedet, aber im letzten Moment auf Druck des Bundesrates noch massiv verschlechtert. Was Gefangene zum Beispiel dem Gefängnispsychologen anvertrauen, muß bereits dann an die Anstaltsleitung weitergegeben werden, wenn es „der Aufgabenerfüllung der Vollzugsbehörde dient". Früher war dies nur zulässig, wenn von einer Person konkret eine Gefahr ausging. Wie unter der neuen Rechtslage überhaupt eine vertrauensvolle Therapie möglich sein soll, bleibt schleierhaft. Gefangenenpersonalakten müssen jetzt 30 Jahre aufbewahrt werden, länger als in fast allen anderen staatlichen Bereichen. Da nützt es den Betroffenen wenig, wenn ihre Daten nach dem Bundeszentralregistergesetz und nach den Polizeigesetzen im Interesse der Resozialisierung schon viel früher gelöscht worden sind (vgl. Tz. 4.4.2).

Positive Gesetzgebungsbeispiele hingegen sind rar. Außer dem **Teledienstedatenschutzgesetz** ist in den vergangenen Jahren kaum ein neuer Impuls aus der Bundesgesetzgebung gekommen. Erste Untersuchungen zur Umsetzung des Gesetzes zeigen allerdings, daß Deutschland in diesem Bereich zwar ein mustergültiges Gesetz hat, das im Ausland gerne bei passender Gelegenheit als überzogen und perfektionistisch vorgeführt wird, daß die Umsetzung des Gesetzes in die Praxis aber weitgehend leerläuft. Es wird häufig nicht beachtet, ist vermutlich vielen Anbietern in den Einzelheiten gar nicht bekannt und den Aufsichtsbehörden und den einzelnen Internetnutzern fehlen die Instrumente, um seine Beachtung durchzusetzen.

Schon seit 1995, also seit drei Jahren, besteht die Notwendigkeit, die allgemeinen Datenschutzgesetze an die Europäische Datenschutzrichtlinie anzupassen. Die Frist verstrich im Oktober 1998, ohne daß die bis dahin schleppend geführte Debatte wenigstens zufriedenstellende Zwischenergebnisse gebracht hätte. Zu einem wirklichen **Neuanfang** in der Datenschutzgesetzgebung konnte sich der Bundesgesetzgeber bislang noch nicht aufraffen; zu einer Fortsetzung des bisherigen Regelungsansatzes hat verständlicherweise offenbar auch niemand so richtig Lust. Die neue Bundesregierung läßt durchblicken, sie wolle in einer ersten Stufe die allernötigsten Konsequenzen aus der Europäischen Datenschutzrichtlinie ziehen, danach dann in der zweiten Stufe eine gründliche Revision des Bundesdatenschutzgesetzes vornehmen. Warum nicht gleich Nägel mit Köpfen gemacht werden sollen, bleibt unerfindlich.

Das Tempo der Novellierungsdiskussion zum **Bundesdatenschutzgesetz** steht geradezu in einem auffälligen Gegensatz zu dem Schwung, mit dem in schöner Regelmäßigkeit direkt im Anschluß an einzelne Straftaten Eingriffsbefugnisse der Polizei verschärft werden. Es steht auch im krassen Widerspruch zu der Dynamik, mit der die Politik die Entwicklung der Informationsgesellschaft pausenlos vorantreibt.

- **Die Informationstechnik**

Dabei bestünde für eine **umfassende Modernisierung** des Datenschutzrechts dringender Bedarf. Die gegenwärtigen Gesetze basieren auf einer technologischen Basis, die schon lange überholt ist. Die Großrechnertechnologie ist in weiten Bereichen längst ersetzt durch vernetzte PC. Nahezu jede Behörde verfügt über Serverkapazitäten, die früher ein respektables Rechenzentrum ergeben hätten, häufig ohne daß das entsprechende professionelle Know-how vorhanden ist. Die Folge sind gravierende Sicherheitsmängel (vgl. Tz. 4.1.2; Tz. 6.1; Tz. 6.2). Chipkarten kennen die Datenschutzgesetze noch gar nicht; trotzdem wird ihr Einsatz in einigen Bereichen erwogen bzw. ausprobiert (vgl. Tz. 4.5.2; Tz. 4.9.3). In keinem Datenschutzgesetz ist die Verschlüsselung geregelt oder gar zur Pflicht gemacht. Datenvermeidung, Datensparsamkeit, Systemdatenschutz und „mehrseitige Sicherheit" finden nur zögerlich auf dem Umweg über das Teledienstedatenschutzgesetz Eingang in das Datenschutzrecht.

Schleswig-Holstein möchte bei der Entwicklung und Nutzung der Informationstechnik offenbar eine führende Rolle spielen. Die Landesregierung spricht davon, Schleswig-Holstein entwickele sich zum Mekka der Informations- und Kommunikationstechnologie. In vielen Reden werden die Chancen der Informationstechnik beschworen. Der Wirtschaftsminister meint, im Netz liege die Zukunft und kündigt an, in den nächsten drei Jahren werde das Land mehr als 40 Millionen Anschubfinanzierung für den Ausbau der Informationsgesellschaft geben.

Viele geplante oder schon begonnene Projekte zeigen, in welchem Ausmaß die Informationstechnik vorangetrieben werden soll. Da ist von „Verwaltung 2000" die Rede, bei der die Verwaltung ihre Leistungen über das Internet erbringen soll, von einer landesweiten Infrastruktur, von der Einrichtung virtueller Marktplätze,

auf denen öffentliche und kommerzielle Angebote gebündelt werden sollen, vom Ausbau der Krankenhausinformationssysteme, von einem Informationsnetz Umwelt, von einem Informationssystem Ostsee-Anrainer-Staaten, von Bürgernetzen, von netzbasierten Bildungs- und Fortbildungseinrichtungen, vom Multimedia-Campus Schleswig-Holstein, von einem Landesinformationssystem Schleswig-Holstein, das alle Internetaktivitäten des Landes bündeln soll und vielen weiteren Vorhaben.

Im Landeshaushalt wird weiterhin kräftig in Informationstechnik investiert. Jahr für Jahr gibt allein das Land mehr als 120 Millionen DM für die IT-Ausstattung der Landesverwaltung aus. Nach dem IT-Gesamtplan wird der Anteil der ausstattungsfähigen Arbeitsplätze, die über Informationstechnik verfügen, von 76,26 % im Jahr 1998 bis zum Jahr 2002 auf 90,34 % gesteigert. Die einzelnen im IT-Gesamtplan aufgeführten Projekte der Ressorts zeigen, daß die Informationstechnik in allen Bereichen der Verwaltung mit ungeheurer Dynamik vorangetrieben wird. In den Kommunen bestehen vergleichbare Planungen, mit denen die Modernisierung und Effektivierung der Verwaltung vorangebracht werden soll.

1.2 Konsequenzen für ein neues Datenschutzrecht

Die **Technik galoppiert** also weiter und läßt bei vielen Bürgerinnen und Bürgern das Gefühl entstehen, der Staat lasse sie beim Schutz ihrer Privatsphäre zunehmend allein. Aus Umfragen ist bekannt, daß sich die Mehrheit einen besseren Datenschutz wünscht. Offenbar fühlen sich viele in offenen Netzen unsicher und agieren entsprechend zurückhaltend. E-Commerce, Online-Banking und anderes läuft im Internet längst nicht so gut wie erwartet, weil die Surfer kein Vertrauen in die Sicherheit des Systems haben. Fehlender Datenschutz als Investitionshindernis – meist liest man es bislang andersherum.

In der **Zangenbewegung** von ständigen zusätzlichen Eingriffsbefugnissen, bei denen die Erfahrungen einzelner Kriminalfälle postwendend in neue Gesetze umgemünzt werden, überholten gesetzgeberischen Ansätzen und einer ungezügelten Technik, deren gesetzgeberische Begleitung eigentlich höchste Aufmerksamkeit erfordern würde, droht das Grundrecht auf informationelle Selbstbestimmung mehr und mehr auszubluten.

Es hat offenbar keinen Zweck, an den Symptomen herumzukurieren. Die Umsetzung der Europäischen Datenschutzrichtlinie darf nicht zu einer linearen Fortsetzung der bisherigen Gesetzgebung führen. Gerade weil das Datenschutzrecht in vielen bereichsspezifischen Verarbeitungsnormen in den vergangenen Jahren durch kurzatmige Gesetzgebungsschritte mehr und mehr verschlechtert worden ist, müssen die allgemeinen Datenschutzgesetze **von Grund auf erneuert** werden. Die Annahme früherer Jahre, viele Datenschutznormen bedeuteten automatisch „viel Datenschutz", hat sich als falsch erwiesen. Wir brauchen schlanke, sachgerechte und zukunftsorientierte Lösungen, die den Kern der Sache wirklich treffen und sich nicht in ausufernden Details verlieren. Der Schutzgedanke der Datenschutzgesetze für Bürgerinnen und Bürger muß wieder mehr im Vorder-

grund stehen.

Als uns der **Schleswig-Holsteinische Landtag** mit Beschluß vom September 1998 aufforderte, ein Gutachten über die Notwendigkeit der Novellierung des Landesdatenschutzgesetzes vorzulegen und dafür konkrete Vorschläge zu machen, haben wir wegen des Umfangs der notwendigen grundsätzlichen Änderungen auf umständliche Prosa verzichtet und unsere Ideen gleich in Form eines **Gesetzentwurfs** unterbreitet. Dabei standen folgende Ziele im Vordergrund:

- Das Gesetz sollte, wo immer dies ohne Verlust für die Rechte der Bürgerinnen und Bürger möglich und unter Berücksichtigung der Europäischen Datenschutzrichtlinie zulässig war, **verschlankt** und **entbürokratisiert** werden. Auf überflüssige Begriffsdefinitionen wurde verzichtet, viele Vorschriften wurden präziser und knapper formuliert. Trotz neuer Elemente, deren Regelung zwingend aus der Europäischen Richtlinie folgt, wie zum Beispiel des Widerspruchsrechts, der Vorabkontrolle, der Datenübermittlung in Staaten außerhalb der EU oder besonderer Vorschriften zu Entscheidungen in automatisierten Verfahren, wurde unser Entwurf kürzer als das bestehende Gesetz.
- Um die ausufernde Normenflut in bereichsspezifischen Gesetzen einzudämmen, wurde für die eher unproblematischen Fälle der Datenverarbeitung in das Gesetz selbst eine bereichsübergreifende Befugnisnorm aufgenommen. Damit soll auch ein spürbarer Beitrag zu den Bemühungen um **Deregulierung** geleistet werden.
- **Neue technische Entwicklungen** wie Dezentralisierung, Vernetzung, Chipkarten, Internet oder Workflow-Management sind berücksichtigt und in angemessenen Formulierungen in den Entwurf integriert. Beim Chipkarteneinsatz wird größter Wert auf Transparenz für die Betroffenen gelegt.
- Die **Technik** soll, wo immer dies möglich ist, zum **Schutz der Grundrechte** eingesetzt werden. Die Bestimmungen zur Datensicherheit sind deshalb gestrafft und präzisiert worden. Datenvermeidung, Datensparsamkeit, Systemdatenschutz und Kryptographie sollen wichtige technische Instrumente für wirksameren Datenschutz werden.
- Der **Modernisierung der Verwaltung** wird Rechnung getragen durch Regelungsvorschläge zum Outsourcing, zur förmlichen Freigabe von IT-Verfahren, zur Kontrolle der Systemadministratoren, zur Telearbeit oder zu Workflow-Konzepten. Verwaltung online, von der vielerorts gesprochen wird, setzt zuallererst Sicherheitsstandards im Internet voraus, die im geltenden Landesdatenschutzgesetz bislang nicht berücksichtigt sind. Beispielsweise ist sicherzustellen, daß die datenschutzrechtliche Einwilligung künftig auch elektronisch erteilt werden kann.
- Der Datenschutz soll sich von einer vornehmlich kontrollierenden und kritisierenden Einrichtung zu einer auch beratenden und **Serviceleistungen** erbringenden Stelle wandeln. Die Einführung eines allgemeinen Datenschutz-Audits soll die Behörden ermuntern, sich vor Ort eigene Datenschutzkonzepte zu erarbeiten, und so die Dezentralisierung und Selbstverantwortung im Datenschutz fördern.

Der Wortlaut unseres Gesetzentwurfs und ein Überblick über die wesentlichen Neuerungen sind im Anhang abgedruckt. Außerdem können der Entwurf, die Begründung, eine Synopse sowie weitere Materialien auf unserer Homepage abgerufen werden:



www.schleswig-holstein.datenschutz.de
(Rubrik: weitere Materialien/Gesetze)

Der Innenminister wurde vom Landtag aufgefordert, einen Bericht über die Zusammenlegung der Datenschutzkontrolle im öffentlichen Bereich und der Datenschutzaufsicht über den Privatbereich vorzulegen. In seinem Bericht schlägt der Innenminister vor, entweder eine oberste Landesbehörde oder eine unabhängige Landesanstalt zu bilden. Die Entscheidung hierüber obliegt dem Parlament. In unserem Gesetzentwurf ist die Zusammenlegung von Aufsicht und Kontrolle sowie das daraus folgende Organisationsmodell deshalb ausgeklammert.

Der Schleswig-Holsteinische Landtag hat unsere Vorschläge im November 1998 diskutiert. Redner aller Fraktionen äußerten sich zustimmend, so daß offenbar gute Chancen bestehen, zu parteiübergreifenden Lösungen zu kommen. Der Innenminister kündigte in der Debatte einen eigenen Gesetzentwurf an. Bei Redaktionsschluß lag uns ein Text für die Abstimmung mit den anderen Ressorts vor.

1.3 Die Arbeit der Dienststelle

Die Bedingungen für den Datenschutz sind wie sie sind. Wir haben uns im vergangenen Jahr bemüht, auf ihrer Grundlage zum Schutz des informationellen Selbstbestimmungsrechts der Bürgerinnen und Bürger so gut wie möglich beizutragen.

- **Der „*neue* Datenschutz" in der Praxis**

Wer Forderungen an andere stellt, muß auch selbst bereit sein, zur Verbesserung der Situation beizutragen. Nicht nur die Gesetze müssen besser werden, auch die Datenschutzpraxis braucht neue Impulse. Die Sommerakademie 1998 hat sich unter dem Titel „Der *neue* Datenschutz" mit einer Fülle von Ideen und Vorschlägen für die Verbesserung des Datenschutzes im Alltag auseinandergesetzt. Vieles davon betraf die Arbeit der Datenschutzbeauftragten selbst. Damit dies nicht alles nur Theorie bleibt, haben wir einige der Ideen, die die Experten bei der Sommerakademie zur Diskussion stellten, **in die Praxis umgesetzt**, soweit dies im Bereich unserer Möglichkeiten lag. Wir konnten dabei gut an Ansätze anknüpfen, die wir in den vergangenen Jahren bereits entwickelt hatten.

Unser Vorschläge zur *Novellierung des Landesdatenschutzgesetzes* machten Ernst mit der Idee, die Verrechtlichung des Datenschutzes auf ein vertretbares Maß zurückzuschrauben. Das Gesetz soll schlanker und präziser werden und das bereichsspezifische Recht spürbar entlasten.

Die Möglichkeiten unseres *IT-Labors* haben wir konsequent für den Test datenschutzfreundlicher Technik genutzt. Referenzinstallationen und praktische Tests haben die Beratungsmöglichkeiten gegenüber Behörden und Bürgern, zum Beispiel zur Verschlüsselung oder zur Einrichtung von Firewalls, spürbar verbessert (vgl. Tz. 7.1.2; Tz. 7.1.3).

Die *Serviceorientierung* unserer Tätigkeit wurde kontinuierlich weiterentwickelt. Ein gemeinsam mit dem Europäischen Verbraucherzentrum herausgegebenes Faltblatt mit dem Titel „Verschlüsseln – Ich?" und eine ergänzend eingerichtete Serviceseite im Internet geben konkrete Tips, wie man sich durch Verschlüsselung gegen fremde Neugier selbst wirksam schützen kann (vgl. Tz. 7.1.3).

Die maßgebliche Mitarbeit in *Modellprojekten* wie „Unbeobachtbarer Netzzugang" oder „Datenschutzgerechte Biometriegestaltung", gemeinsam mit Herstellern und Entwicklern, gibt uns endlich die Möglichkeit, Datenschutzgesichtspunkte in neue Großprojekte schon von Anfang an einzubringen (vgl. Tz. 7.1.1; Tz. 7.2).

Die seit Jahren erfolgreiche *Beratung* in den Kursen der DATENSCHUTZ-AKADEMIE wird immer mehr durch die zeitaufwendige Begleitung konkreter IT-Projekte ergänzt. Die Projektgruppen, in denen wir von Anfang an mitarbeiten und so praktische Technikfolgenabschätzung und präventiven Datenschutz Hand in Hand gehen lassen, belaufen sich auf Dutzende. Das ist enorm zeitaufwendig, kaum spektakulär, aber ungemein effektiv.

- **Die Kontrollen**

All dies ist nicht zu Lasten der Kontrollen vor Ort gegangen. Auch im Berichtsjahr haben sich Zahl und Qualität unserer Kontrollbesuche kaum verändert. Es hat sich gezeigt, daß man immer häufiger auf einzelne Behörden trifft, die die datenschutzrechtlichen Regeln beherrschen und anwenden. Andererseits sind die festgestellten **Mängel** nach wie vor **erschreckend** (vgl. Tz. 4.1.2). Vielleicht macht den Verantwortlichen das Zittern um die Jahr-2000-Problematik klar, daß eine sichere, ordnungsgemäße Datenverarbeitung langfristige Vorteile bietet, die weit über den Tag hinausreichen.

Besonders bedenklich stimmt, daß gerade dort, wo besonders sensible Daten verarbeitet werden, die festgestellten Mängel sich häuften. Eine Kontrolle im Städtischen Krankenhaus in Kiel zeigte erneut, daß die Sicherheitsprobleme bei der automatisierten Speicherung von **Patientendaten** in vielen Krankenhäusern nicht gelöst sind. Die Faszination für die schnelle Verfügbarkeit von Gesundheitsdaten verstellt den Blick auf die Frage, welcher Beweiswert beispielsweise Computerspeicherungen zukommt, wenn sich Patient und Arzt oder Krankenhaus über die Behandlung streiten. Solange der Manipulation von Computerdokumentationen Tür und Tor geöffnet sind, haben beide, Patient und Arzt, Nachteile (vgl. Tz. 6.7.3).

Daß die Datenschutzbestimmungen bei der AOK Schleswig-Holstein so eklatant mißachtet würden, konnten wir zu Beginn unserer Prüfung nicht ahnen. Was Diskretion und Rücksichtnahme auf die Belange der Kunden angeht, sind die Banken inzwischen offenbar weiter als diejenigen, die mit **Sozial- und Patientendaten** umgehen. Optimistisch stimmt allerdings, daß der AOK-Vorstand nach unserer Kontrolle nicht lange um den heißen Brei herumgeredet hat, sondern die Mängel zügig beseitigen will. Bis September 1999 soll alles so weit in Ordnung sein, daß die AOK auch für andere Kassen ein Vorbild ist (vgl. Tz. 4.7.2; Tz. 6.7.1).

- **Die Beratung**

Die Kontrollen gehen immer häufiger nahtlos in Beratungen über. Da wir unsere Beanstandungen nie ohne **Verbesserungsvorschläge** aussprechen, wird den geprüften Stellen klar, daß das Anprangern von Mängeln kein Selbstzweck ist. Statt zigtausend DM für sündhaft teure Beratungsgutachten auszugeben, lassen sie sich detaillierte Expertisen aus unserer Dienststelle geben. Dagegen ist nichts zu sagen, wenn jedem klar ist, in welchem Umfang inzwischen die Kapazität der Dienststelle für Beratungen „zum Nulltarif" in Anspruch genommen wird. So manche Kommune entlastet ihren Haushalt auf diesem Wege still und leise ganz beträchtlich, was den Bürgerinnen und Bürgern ebenfalls zugute kommt.

Daneben haben wir uns bemüht, Notwendigkeit und Wirkungsweise des Datenschutzes auf den verschiedensten Wegen publik und populär zu machen. Neben den vielen Kursen der DATENSCHUTZAKADEMIE, für deren Bedarf offenbar kein Ende absehbar ist, hat sich die Sommerakademie zu einem Anziehungspunkt für Datenschutzexperten aus dem ganzen Bundesgebiet entwickelt. In circa einem Dutzend Pressekonferenzen in Kiel und Bonn wurden der Öffentlichkeit aktuelle Themen vorgestellt, in ebenso vielen Presseerklärungen datenschutzrechtliche Argumentation verbreitet und für eine Verbesserung des Datenschutzes der Bürgerinnen und Bürger geworben. Die Zahl der Vorträge, die die Mitarbeiterinnen und Mitarbeiter auf Kongressen und Veranstaltungen in Schleswig-Holstein und im Bundesgebiet gehalten haben, geht ebenfalls in die Dutzende. Daneben setzen sich viele in ihrer Freizeit hin und versuchen in wissenschaftlichen Veröffentlichungen die datenschutzrechtliche Diskussion mitzubestimmen. Alles in allem ein „volles Programm", das keine weiteren Spielräume mehr läßt. Wer „mehr Datenschutz" möchte, der muß mehr investieren.

2. Der Weg in die Informationsgesellschaft

2.1 Fernmeldegeheimnis und Telekommunikation

Das Brief-, Post- und Fernmeldegeheimnis gehört zu den traditionellen Garantien einer freiheitlichen Verfassung. Artikel 10 Grundgesetz gewährleistet nach der Rechtsprechung des Bundesverfassungsgerichts die freie Entfaltung der Persönlichkeit durch einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Informationen und wahrt damit die Würde des denkenden und freiheitlich handelnden Menschen. In seiner **grundlegenden Schutzfunktion** wurde Artikel 10 Grundgesetz trotz der Beschränkungen durch das G 10-Gesetz aus dem Jahre 1968 seit Inkrafttreten des Grundgesetzes nicht geändert.

Geändert haben sich aber die **realen Bedingungen** des Brief-, Post- und Fernmeldeverkehrs, der sich im Zeitalter der internationalen Vernetzung zu einem umfassenden Datenaustausch entwickelt hat. Nicht nur die Zahl der Kommunikationsvorgänge hat rapide zugenommen, sondern auch die Qualität und Sensibilität der ausgetauschten Informationen. Kaum ein Lebensbereich, von der Versorgung mit Nachrichten über die Erledigung von Bank- und sonstigen Geschäften, über die Telemedizin bis hin zur Eheanbahnung und zur Erbringung von Arbeitsleistungen in Form von Telearbeit, der nicht „online" erledigt werden könnte. Die virtuelle Netzwelt wird immer mehr Abbild und Ersatz der realen Welt. Die Politik fördert diese Entwicklung nach Kräften, getrieben von der Angst, anderenfalls könnte der wirtschaftliche oder welcher Anschluß auch immer verpaßt werden. Schulen, Universitäten, Banken, Krankenhäuser, Verwaltungsbehörden, eben praktisch alle sollen so schnell wie möglich „ans Netz".

Gemeint ist in aller Regel das Internet, ein liebenswürdig-chaotisches Gebilde, das vieles bietet, nur eines nicht: Sicherheit und Vertraulichkeit. Im Gegensatz zur realen Welt gibt es im Internet kaum eine anonyme Transaktion. Auch sensibelste Daten werden, nicht anders als Belangloses und Banales, offen verbreitet, wenn nicht besondere Sicherheitsvorkehrungen getroffen werden. Da im Zuge der **Privatisierung** der Telekommunikation der Staat sein Post- und Fernmeldemonopol verloren hat, können Sicherheit und Wahrung der Vertraulichkeit gegenüber den vielen neuen Telekommunikationsanbietern auch nicht einfach per Gesetz und Verordnung durchgesetzt werden. Dies um so weniger, als Datennetze international sind und sich dem Zugriff nationaler Gesetzgebung weitgehend entziehen.

Die klassische Konstellation des Artikels 10 Grundgesetz, wonach die Post als Sachwalter der Bürger vor der Neugier anderer staatlicher Stellen zu schützen ist, existiert nicht mehr. Auch die privatrechtlich vermittelte Telekommunikation bedarf weiterhin des Schutzes gegen staatliche Abhörwünsche. **Artikel 10** Grundgesetz ist als **Abwehrgrundrecht** gegen staatliche Eingriffe in das Fernmeldegeheimnis also keineswegs überflüssig geworden.

Damit sind die Bürger aber **nicht ausreichend** geschützt, denn es bleiben die Eingriffsmöglichkeiten der privaten Telekommunikationsbetreiber selbst und die unbefugter Dritter, seien es Hacker oder fremde Geheimdienste. Die Gesetzgebung hat zwar die Telekommunikationsanbieter zur Wahrung des Fernmeldegeheimnisses gesetzlich verpflichtet und nach wie vor ist das unbefugte Abhören des Fernmeldeverkehrs strafbar; das genügt aber für den Schutz der Bürger nicht. Schon die Internationalität der Datenströme zeigt die Begrenztheit derartiger Verbotsnormen. Welcher ausländische Geheimdienst, welche international organisierte Verbrecherbande, welcher Hacker in – sagen wir Neuseeland – wird sich von einem deutschen Abhörverbot beeindrucken lassen?

Die Veränderungen in der Telekommunikation verlangen erweiterte Schutzgarantien für das Brief-, Post- und Fernmeldegeheimnis. Die bloße Abwehr staatlicher Eingriffe genügt nicht mehr. Vielmehr müssen ergänzend staatliche Maßnahmen zum Schutz der in Artikel 10 Grundgesetz aufgeführten Geheimnisse gegen neugierige Dritte hinzutreten. Notwendig sind nicht nur Ge- und Verbote, sondern **wirksame technische Vorkehrungen**. Eine davon ist die effektive **Verschlüsselung** von Daten, die in offenen Netzen übertragen werden. In Deutschland ist die Verschlüsselung bislang gesetzlich nicht eingeschränkt (vgl. Tz. 7.4). In der Praxis wird von ihr allerdings noch wenig Gebrauch gemacht. Sie erscheint kompliziert und als lästige Zusatzaufwendung. Wegen der andauernden Kryptodebatte (vgl. Tz. 7.7) haftet ihr der Geruch einer unlautere Machenschaften vortäuschenden Maßnahme an. Im Ergebnis ist jedenfalls der Datenverkehr im Internet zum größten Teil gegen unbefugtes Mitlesen, Kopieren, Verändern oder Löschen nicht gesichert. Der E-Mail-Verkehr gleicht der traditionellen Post, nur leider ohne Briefumschlag.

Da Artikel 10 nach der Rechtsprechung des Bundesverfassungsgerichts nicht nur ein Abwehrgrundrecht ist, sondern ein **objektives Ordnungsprinzip** enthält, muß sich die staatliche Verpflichtung zur Grundrechtsgewährung vom bloßen Unterlassen von Eingriffen hin zu Beratungs- und Unterstützungspflichten gegenüber den Bürgern weiterentwickeln, damit diese sich selbst wirksam schützen können. Denkbar ist beispielsweise das staatliche Werben für starke Verschlüsselungsverfahren und die Bereitstellung von Servicefunktionen für die Verschlüsselung in der täglichen Praxis.

Bislang mußte man allerdings im Gegenteil befürchten, daß sogar das Recht auf Verschlüsselung zugunsten der staatlichen Sicherheitsbehörden eingeschränkt würde. Die Politik der Bundesregierung war in den vergangenen Jahren einseitig darauf ausgerichtet, im Zuge der Privatisierung der Telekommunikation auf keinen Fall Einbußen bei den staatlichen Abhörmöglichkeiten zuzulassen (vgl. Tz. 7.8). Die erklärte Absicht, nur ja **keine „abhörfreien Räume"** in der Telekommunikation entstehen zu lassen, führte zu einer kontinuierlichen Ausweitung der staatlichen Abhör- und Überwachungsmöglichkeiten bis hin zu grotesken Exzessen. Würden beispielsweise die in dem letzten Entwurf der Telekommunikationsüberwachungs-Verordnung vorgesehenen Verpflichtungen für alle Provider, Vorsorge für etwaige staatliche Überwachungswünsche zu treffen, tatsächlich realisiert, wären nach Schätzungen der Betroffenen Investitionen von über

40 Milliarden DM erforderlich, für die letztlich über Leistungsentgelte am Ende die Kunden, also die Überwachten selbst, aufzukommen hätten.

Die durch die Proteste der Telekommunikationsanbieter gegen den Verordnungsentwurf erzwungene Atempause sollte genutzt werden, um die einseitige Ausrichtung der staatlichen Telekommunikationspolitik in Deutschland auf Überwachung und Kontrolle zu beenden und statt dessen den legitimen und grundrechtlich geschützten Anspruch der Bürgerinnen und Bürger auf **unbeobachtbare Kommunikation** wieder in den Mittelpunkt zu rücken. Noch fehlt der Politik in Deutschland offenbar das Gespür für die überragende Bedeutung geschützter Telekommunikation unter den Bedingungen der neuen Informationsgesellschaft. Ein Abrücken von den Gedankenspielen über Möglichkeiten zur Einschränkung der Verschlüsselungsfreiheit allein genügt nicht. Notwendig sind vielmehr aktive Schritte zur Verbesserung des Schutzes der Privatsphäre in Netzen wie z. B.

- aktive Förderung der Verschlüsselung durch Privatpersonen und Wirtschaftsunternehmen;
- Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern;
- Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen wie Ärzten, Anwälten, Psychologen usw.;
- Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer Betriebsgeheimnisse gegen Abhörversuche ausländischer Geheimdienste;
- Förderung von Projekten, die den Bürgerinnen und Bürgern das anonyme Surfen im Internet ermöglichen;
- Verbot von Geräten und Systemen, die ausschließlich zum unbefugten Abhören fremder Telekommunikation bestimmt sind;
- konsequente Anwendung der Bestimmungen zum Schutz des Fernmeldegeheimnisses und Verbesserung der Telekommunikationsgesetze.

2.2 Frist für die Umsetzung der Europäischen Datenschutzrichtlinie verpaßt

Am 24. Oktober 1995 wurde die „Richtlinie der Europäischen Union zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" im Amtsblatt der Europäischen Gemeinschaften verkündet. Die Mitgliedstaaten hatten drei Jahre Zeit, ihr Datenschutzrecht an die Richtlinie anzupassen. Weder im Bund noch in den Ländern (außer Hessen und Brandenburg) wurde es aber bislang novelliert. Auch **Schleswig-Holstein** hat die **Frist nicht eingehalten**. Nunmehr sind Sanktionen der Europäischen Union nicht ausgeschlossen. Außerdem stellt sich die Frage, welche Teile der Richtlinie unmittelbare Geltung haben. Da insoweit auch Europarechtsexperten uneins sind, wächst die Verunsicherung darüber, in welchem Umfang das geltende Landesdatenschutzgesetz von unmittelbar anwendbaren Bestimmungen der Richtlinie über-

lagert wird.

Daß die Umsetzung der Richtlinie in drei Jahren nicht bewältigt werden konnte, kann nicht nachdrücklich genug kritisiert werden, zumal der „Rat für Forschung, Technologie und Innovation der Bundesregierung" bereits im Dezember 1996 in seinen Empfehlungen unmißverständlich klargestellt hatte, daß ein „konsequenter Datenschutz" zu den **zentralen Akzeptanzvoraussetzungen** der Informationsgesellschaft zählt. Offenbar mißt die Politik, wenn es um die Schaffung der Informationsgesellschaft geht, mit zweierlei Maß: Wenn die technische Infrastruktur zur Debatte steht, überschlägt sich das Vokabular geradezu mit Beschleunigungsfloskeln. Alles muß so schnell wie möglich ans Netz, kein Anschluß darf verpaßt werden, es gilt, keine Zeit gegenüber der Konkurrenz in Übersee zu verlieren, alle müssen schleunigst fit gemacht werden für die Informationsgesellschaft usw. Geht es um die notwendige **soziale** und **rechtliche Infrastruktur**, macht sich eine merkwürdige Zurückhaltung breit. Die Gesetzgebung kommt jahrelang nicht voran. Die Debatte über die datenschutzrechtliche Begleitmusik zur Informationsgesellschaft wird hinhaltend und ohne Schwung geführt.

Dabei wurden in Deutschland schon Erfahrungen mit anderen Großtechnologien gemacht, die ohne die Akzeptanz der Menschen auf Dauer keine Chancen haben. Zwar erwarten sich viele Nutzer von den Computern Hilfe und Erleichterung und wissen sie als willkommene Freizeitbeschäftigung zu schätzen. Aber wenn es ums Geld geht, beim **E-Commerce** über Internet beispielsweise, zeigen sie eine von großer Skepsis getragene Zurückhaltung. Die tatsächlichen Nutzerzahlen in diesem Bereich bleiben weit hinter den hochgesteckten Erwartungen und den Hochglanzgrafiken zurück. Aus Umfragen in der Europäischen Union und in Amerika kennen wir den Grund: Die Menschen haben **kein Vertrauen** in die Sicherheit des Internets. Sie befürchten die Ausspähung ihrer Privatsphäre und im schlimmsten Fall auch Opfer von Straftaten zu werden. Offenbar ist es ein Fehler zu glauben, die Nutzer würden im Internet geldrelevante Transaktionen genauso unbefangen vornehmen wie das Absurfen von Informationen oder das Chatten über Gott und die Welt.

Das Versäumen der Frist zur Umsetzung der EU-Richtlinie zeigt einmal mehr, daß die Politik selbst bei ihren Vorbereitungen auf die Informationsgesellschaft und insbesondere bei der Gestaltung der sozialen und rechtlichen Rahmenbedingungen beileibe noch nicht so „fit" ist, wie sie dies von anderen erwartet.

3. Datenschutz im Landtag

3.1 Endlich eine Datenschutzordnung für den Landtag

Der Landtag hat sich eine Datenschutzordnung gegeben, die sich sehen lassen kann: Danach bedarf es auch bei der Verarbeitung personenbezogener Daten für parlamentarische Zwecke der Berücksichtigung der schutzwürdigen Interessen der Betroffenen. Bei der Bearbeitung von Petitionen, in Immunitätsangelegenheiten, bei der Beweiserhebung durch Untersuchungsausschüsse oder soweit besondere Amts- und Berufsgeheimnisse betroffen sind, sind die Daten besonders vertraulich zu behandeln. Die Datenweitergabe für die wissenschaftliche Forschung ist geregelt und auch die Übermittlung an Private, die ein rechtliches Interesse glaubhaft gemacht haben. Den Betroffenen wird nicht nur ein Auskunftsanspruch eingeräumt, sondern auch ein Recht auf Richtigstellung unwahrer personenbezogener Angaben in Landtagsdrucksachen. Zu Beginn jeder Wahlperiode wird ein **Datenschutzgremium** gebildet, dem alle Fraktionen angehören und das die Beachtung des Datenschutzes im Parlamentsbereich überwacht. Es nimmt Beschwerden und Beanstandungen betroffener Bürgerinnen und Bürger entgegen und geht diesen Vorgängen nach.

Leider verbleiben für die künftige Praxis noch Unsicherheiten. So ist, entgegen dem ursprünglichen Entwurf, ungeklärt, wie Betroffene ihre Datenschutzrechte gegenüber den **Landtagsfraktionen** wahrnehmen können. Sie sind lediglich verpflichtet, die Umsetzung der Datenschutzordnung „in eigener Verantwortung sicherzustellen". In den Regelungen über die technischen und organisatorischen Maßnahmen werden die Fraktionen gar nicht erwähnt. Selbstverständlich können aber die Fraktionen nicht von ihren Pflichten gegenüber den Betroffenen freigestellt werden. Es bleibt daher die Frage offen, ob insoweit das für private Stellen geltende Bundesdatenschutzgesetz anwendbar und die Aufsicht vom Innenministerium als Datenschutzaufsichtsbehörde wahrzunehmen ist.

3.2 Behindert Datenschutz die Information der Abgeordneten?

Bei parlamentarischen Anfragen zu politisch unangenehmen Sachverhalten wird nicht selten der Datenschutz zur Rechtfertigung einer Auskunftsverweigerung bemüht. So hat z. B. die Landesregierung auf eine Kleine Anfrage nach den Namen von Gutachtern und den Kosten der im Auftrag des Landes erstellten Gutachten die Antwort mit dem Hinweis auf „den Datenschutz" verweigert. Wir haben dies zum Anlaß genommen, die **Grenzen des parlamentarischen Fragerechts** auszuloten.

Die Landesverfassung legt in ihrem Artikel 23 fest, daß die Beantwortung von Fragen nur in ganz engen Grenzen abgelehnt werden kann, z. B. wenn dem Bekanntwerden des Inhalts von Akten schutzwürdige Interessen einzelner, insbesondere des Datenschutzes, entgegenstehen. Dem verfassungsrechtlich abgesicherten **Informationsrecht des Parlaments** und dem Öffentlichkeitsgrundsatz der Landtagsberatungen steht also das Datenschutzinteresse natürlicher Personen gegenüber. Beides dient der Kontrolle der Verwaltung im Rahmen der Gewaltenteilung und zur Schaffung einer größtmöglichen Transparenz für die Bürgerinnen und Bürger. Zwischen diesen gegenläufigen Interessen muß ein verfassungskonformer Ausgleich vorgenommen werden. Dem widerspricht eine pauschale Informationsverweigerung unter Verweis auf „den Datenschutz".

Schutzwürdig sind individuelle Geheimhaltungsinteressen dann, wenn sie gegenüber den Informationsinteressen des Parlaments überwiegen. Selbstverständlich ist die Regierung nicht gehindert, vor der Auskunftserteilung die Betroffenen zu informieren und deren **Einwilligung** einzuholen. Ein solches Vorgehen ist sogar zu begrüßen, da dadurch evtl. bestehende schutzwürdige Interessen bekannt werden können. Kann eine Einwilligung nicht erlangt werden oder wird diese gar definitiv verweigert, so darf selbst dies nicht automatisch zur Auskunftsverweigerung führen. Die Landesregierung bleibt weiterhin verpflichtet, die bestehenden Interessen abzuwägen. Dabei ist auch zu berücksichtigen, wie die dem Parlament vorgelegten Informationen weiter behandelt werden. Je nach konkreter Fallkonstellation kommt eine nichtöffentliche Erörterung in Betracht, wenn die Belange der Betroffenen dies gebieten.

Im konkreten Fall war die **namentliche Nennung der Gutachter** und die Höhe der Gutachterkosten für die politische Bewertung und die öffentliche Haushaltskontrolle in der Tat von Bedeutung. Eine besondere persönlichkeitsrechtliche Sensibilität der zunächst vorenthaltenen Angaben war demgegenüber nicht zu erkennen.

3.3 Aufbau des Informations- und Kommunikationssystems

Die Ende 1997 gegründete Arbeitsgruppe aus Mitarbeitern des IT-Referates der Landtagsverwaltung und unseres Technikreferates hat sich im abgelaufenen Jahr intensiv mit den technischen und organisatorischen Fragestellungen beschäftigt, die sich aus der Schaffung eines Informations- und Kommunikationssystems für den Gesamtbereich des Landtages ergeben. Dabei zeigte sich, daß die **Sicherheitsbedürfnisse der einzelnen Benutzer** (z. B. die Landtagsverwaltung im engeren Sinn, der wissenschaftliche Dienst, der stenographische Dienst, die Pressestelle einschließlich der Landespressekonferenz, die Beauftragten, die Fraktionen und die Abgeordneten) nur dann hinreichend befriedigt werden können, wenn zuvor eine sorgfältige Bestandsaufnahme ihrer derzeitigen und für die nächste Zeit geplanten informationstechnischen Aktivitäten und Kommunikationsbedürfnisse durchgeführt wird.

Ein besonderes Augenmerk ist dabei auf die **verfassungsrechtliche Sonderstellung** des „Präsidenten des Schleswig-Holsteinischen Landtages" als Organ des Landtages und gleichzeitig als oberste Landesbehörde sowie auf die der Abgeordneten, der Fraktionen und der Presse zu richten. Dies wurde deutlich, als sich die Arbeitsgruppe mit der Frage befaßte, ob und in welchem Umfang technische Systeme des Innenministeriums und der Datenzentrale in Anspruch genommen werden können. Im Gegensatz zu den Bedingungen in den „klassischen" Ressorts und den ihnen nachgeordneten Behörden erwiesen sich die Sicherheitsanforderungen und Abschottungsnotwendigkeiten der vergleichsweise kleinen Organisationseinheit „Landtag" als ausgesprochen komplex und heterogen. Die Analysen der Dienstleistungsangebote des Innenministeriums und der Datenzentrale sind noch nicht abgeschlossen, haben aber bereits jetzt gezeigt, daß nur eine umfassende Transparenz ihrer Funktionalitäten und genau spezifizierte Vereinbarungen den Sicherheitsstandard gewährleisten, der in diesem hochsensiblen Bereich als erforderlich und angemessen anzusehen ist.

4. Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Überblick

Viele Anzeichen deuten darauf hin, daß in den nächsten Jahren in der kommunalen Welt kaum ein Stein auf dem anderen liegen bleiben wird. Die stetige Erweiterung der Aufgabenstellungen und der gleichzeitig steigende Druck, sich den Bürgern als **hochflexibles** und **modernes Dienstleistungsunternehmen** zu präsentieren, bedingen grundlegend neue Ansätze bei der Gestaltung der kommunalen Aufbau- und Ablauforganisation. Experimentierklauseln in Gesetzen, Kooperationsmodelle, Privatisierungen, Einbindung externer Dienstleister in Form des Outsourcing, Rezentralisierung von IT-Systemen, interaktive Teilnahme der Bürger an Prozessen der kommunalen Selbstverwaltung, Erweiterung der Kontrollkompetenzen der Selbstverwaltungsorgane usw. sind mehr als nur Schlagworte. Sie sind in einigen Bereichen schon Realität.

Deshalb und weil praktisch alle Einwohner dieses Landes von dieser Entwicklung betroffen sind, bedarf sie einer intensiven konstruktiv-kritischen datenschutzrechtlichen Begleitung, damit die **Bürgerrechte** bei der Umsetzung dieser **Modernisierungsmaßnahmen** nicht auf der Stecke bleiben. Die Transparenz der Datenverarbeitung und die Möglichkeiten des Informationszuganges sind zu gewährleisten. Dies hat bereits auf der Ebene der Gesetzgebung und bei der Abfassung interner Verwaltungsvorschriften zu geschehen (Tz. 4.1.4). Außerdem müssen möglichst frühzeitig technische und organisatorische Fehlentwicklungen erkannt und Vorschläge zur Abhilfe unterbreitet werden. Die Grundsatzfragen können zwar am „grünen Tisch" erörtert, die Verwaltungswirklichkeit muß jedoch vor Ort erfaßt und bewertet werden. Aus diesem Grund stand der Bereich „Kommunales" im abgelaufenen Jahr erneut im Zentrum unserer Aktivitäten (vgl. Tz. 4.1.2). Er bindet zur Zeit mehr als ein Drittel unserer personellen Kapazitäten.

4.1.2 Licht und Schatten bei der Datensicherheit im kommunalen Bereich

Mehr und mehr Kommunen bekommen ihre automatisierte Datenverarbeitung gut in den Griff. Der Anteil der mit Sicherheitsmängeln behafteten Systeme ist aber nach wie vor groß. Chefs und Administratoren ohne Durchblick entwickeln sich mehr und mehr zu Sicherheitsrisiken.

Neben den unter Textziffer 4.12 dargestellten „Angemeldeten/Unangemeldeten Kontrollen", bei denen wir auch einen Blick auf die Technik werfen, reicht unsere personelle Kapazität leider nur aus, um jährlich **15 bis 20 umfassende Prüfungen** der Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung im kommunalen Bereich durchzuführen. Bei unveränderten Rahmenbedingungen werden wir also frühestens in 10 Jahren eine Flächendeckung erreicht haben. (Dringend notwendige Wiederholungsprüfungen noch nicht eingerechnet.)

Das Fazit der diesjährigen Prüfungen kann man umschreiben mit „**Licht und Schatten**". Bei der Vorstellung des 20. Tätigkeitsberichtes im Frühjahr 1998 konnten wir mit der Neuigkeit aufwarten, daß gerade der ersten Kommune im Lande bescheinigt werden konnte: „Keine wesentlichen sicherheitstechnischen Beanstandungen, alles o. k.". Erfreulicherweise hat sich dieser Trend fortgesetzt. Zwischenzeitlich haben **mehrere Kommunen** dieses **Testat** von uns erhalten. Dabei ist signifikant, daß die positiven Ergebnisse nicht daraus resultierten, daß die betreffenden Verwaltungen alle die gleiche Checkliste, Vordrucksammlung oder Musterlösung genutzt hatten. Auch die getroffenen Sicherheitsmaßnahmen ließen sich nicht alle über einen Leisten schlagen; sie waren genauso unterschiedlich wie die Zielrichtungen der automatisierten Verfahren, die personellen Situationen und die organisatorischen Rahmenbedingungen. Wir können die vorgefundenen Lösungen also auch nicht als „kopierfähige" Beispiele anbieten.

Worin lag also die **Ursache für die guten Ergebnisse**? Gemeinsam war allen, daß

- die Absichten von den Verantwortlichen klar definiert worden sind,
- jede getroffene Maßnahme einen für alle Beteiligten erkennbaren Sinn und Zweck erkennen ließ,
- Sicherheit und Ordnungsmäßigkeit als nutzbringende, mithin positiv zu bewertende Ziele der Automationsvorhaben angesehen wurden,
- erst geplant und dann Fakten geschaffen wurden,
- nicht woanders „blind" abgeschrieben, sondern paßgenau eigene Lösungen entwickelt wurden, nachdem man sich bei anderen Kommunen „schlau" gemacht hatte, und
- verbliebene Probleme nicht kaschiert, sondern für alle Beteiligten transparent gemacht wurden; dies förderte offenbar die Phantasie für die Entwicklung in der Regel verblüffend einfacher Lösungen in den folgenden Ausbaustufen der Verfahren.

Die Aufzählung zeigt, daß es recht schwer ist, allgemein zu beschreiben, was im einzelnen getan wurde. Weniger erfreulich, aber sehr viel einfacher ist dagegen die Darstellung der Dinge, die den Schatten der automatisierten Datenverarbeitung repräsentieren. Hier gilt es zunächst auf die Aufstellung der Mängel im 20. Tätigkeitsbericht (Tz. 6.7.4) zu verweisen. All dies haben wir auch im abgelaufenen Jahr vorgefunden. Hinzu kamen folgende **„Highlights" im negativen Sinn**:

- Mitarbeiter, die nominell als **Systembetreuer** tätig waren, kannten nicht einmal die entsprechenden Benutzerkennungen und Paßwörter ihrer Systeme. Sie hätten beim Ausfall des regulären Wartungstechnikers nicht einmal von woanders Hilfe bekommen können, denn ohne Benutzerkennung und Paßwort ist jeder Reparaturversuch zum Scheitern verurteilt.
- Die Systemadministration erfolgte ausschließlich durch **externe Dienstleister**, ohne daß die Mitarbeiter der Behörde eine Ahnung davon hatten, „was da so

läuft". In diesen Fällen hätten die „Externen" Administrationsfehler, z. B. falsche Zugriffsberechtigungen, Einspielung falscher Software-Versionen, Nutzung falscher Sicherungskopien, nachträglich kaschieren können, ohne daß eine Chance bestanden hätte, dies zu bemerken.

- Der **Systemzugang** zu einem Zentralrechner war nicht einmal durch ein Paßwort abgesichert. Jeder Nutzer hätte ihn also beliebig manipulieren können. Je unauffälliger die Manipulation, desto unwahrscheinlicher wäre ihre Entdeckung gewesen.
- Zugangsberechtigungen auf dem **Zentralrechner** waren vor Jahren von Lieferanten vergeben worden, sie wurden von den Administratoren der datenverarbeitenden Stelle nie wieder geändert. Der Kreis der „Mitwisser" war mittlerweile riesig. Auch in diesem Fall war der Manipulation, Vernichtung oder Verfälschung der Datenbestände Tür und Tor geöffnet.
- Administratoren verfügten über völlig **unzureichende Systemkenntnisse**. Da Betriebssysteme in der Regel so ausgeliefert werden, daß „alles möglich ist", können wirksame Abschottungsmaßnahmen nur bei entsprechenden Systemkenntnissen getroffen werden. Unbefugte hätten sich die einladenden Optionen der Betriebssysteme zunutze machen können.
- Vorgesetzte gewährten für die Administration „großzügig" einen Anteil von 5 % der Gesamtarbeitszeit der Mitarbeiter. Das machte täglich 24 Minuten aus. Solange dauerte wahrscheinlich die Anfertigung der Sicherungskopien der Datenbestände. Administrationsarbeiten „**zwischen Tür und Angel**" sind eine sehr häufige Ursache für Verarbeitungsfehler, die dann als „menschliches Versagen" hingestellt werden.
- Ein Administrator bestand aus unerfindlichen Gründen darauf, daß ihm die **Paßworte aller Mitarbeiter** bekanntgegeben wurden. Dies deute auf Defizite bezüglich seiner Fachkenntnisse hin. Die Paßworte waren damit wirkungslos, denn jede protokollierte Aktivität hätte nicht nur vom registrierten Benutzer, sondern auch vom Administrator unter einer falschen Kennung stammen können.
- In einem Fall wurden den Mitarbeitern die **Paßworte** per Telefon **zentral vergeben**, vermutlich, um eine gewisse „Einheitlichkeit" zu erreichen. Wenn Paßworte „vergeben" werden, verlieren sie ihren Sinn, da dann stets mindestens zwei Personen davon Gebrauch machen könnten. Eine eindeutige Zuordnung von Rechneraktivitäten ist nicht mehr möglich.
- Man „sicherte" **Diskettenlaufwerke** noch mit Schlössern, als man längst wußte, daß diese defekt und damit wirkungslos waren. Der Verwaltungschef ging von einem virensicheren System aus, als womöglich über Computerspiele und dergleichen eingeschleppte Viren, Bomben und trojanische Pferde schon lange den Computer infiziert hatten. Ohne deren rechtzeitige Entdeckung hätte großer Schaden auf die Kommune zukommen können.
- Aus Sicherheitsgründen „vorsorglich" deaktivierte Diskettenlaufwerke konnten von jedermann wieder angeschaltet werden, weil der Administrator nicht wußte, wie man die entsprechenden **Systemdateien** durch Paßworte schützt.

Wer als Administrator über so geringe Fachkenntnisse verfügt, läuft Gefahr, auch andere Sicherheitsmängel nicht zu entdecken. Den Mitarbeitern wäre es möglich gewesen, auch sensible Datenbestände auf Diskette zu ziehen und unauffällig aus dem Dienstgebäude zu bringen.

- Wegen der praktischen „Einheitlichkeit" erhielten alle Mitarbeiter einen **Schlüssel** für das **Diskettenschloß** ihres PC. Auch ein Arbeitsplatzwechsel brachte keine Probleme mit sich, da alle Schlüssel überall paßten. Derartige „Lösungen" lassen Zweifel an der Seriosität der handelnden Personen aufkommen; man muß befürchten, daß auch in anderen Bereichen Datensicherheit gar nicht gewollt war. Der „Schutz" durch das Diskettenschloß war praktisch wertlos.

- **Netzwerkdrucker** und **Kopierer** waren in einem für das Publikum jederzeit zu betretenden Raum installiert, Fehldrucke und Fehlkopien wurden in einem blauen Sack neben den Geräten gesammelt. Immer wieder berichten Datenschützer und Presse über Fahrlässigkeiten beim Umgang mit Papierschrott; hieraus keine Konsequenzen zu ziehen und es statt dessen „darauf ankommen zu lassen", grenzt an grobe Fahrlässigkeit.

- Pech hatte eine Behörde, der zum Zeitpunkt unserer Prüfung gerade die einzige Mitarbeiterin, die Administrationsaufgaben erledigen konnte, „weggelaufen" war. Mangels **ordentlicher Dokumentation** konnte niemand wissen, ob das System bis zum letzten Tag korrekt administriert wurde. Der Nachfolger, der vielleicht erst nach Wochen oder Monaten gefunden worden ist, wird ein schweres Erbe angetreten haben.

- In vielen Fällen wurden die Arbeiten der **Administratoren** nicht **protokolliert.** Welche Zugriffsbefugnisse zum Beispiel am Vortag, in der abgelaufenen Woche, vor einigen Monaten, im letzten Jahr usw. vergeben worden waren, ließ sich definitiv nicht rekonstruieren. Wenn Täter sich diese Defizite gezielt zunutze machen, können Betrügereien kaum nachgewiesen werden.

- In einigen Behörden konnten die Mitarbeiter auch Datenbestände anlegen, in die niemand anderes (vor allem nicht die Vorgesetzten) Einsicht nehmen konnte. **„Schwarze Listen"** hieß so etwas in der papierenen Welt und war streng verboten. Meistens beginnt derartige, durch den Spieltrieb der Mitarbeiter entfachte privat-/dienstliche Datenverarbeitung ganz harmlos. Wenn Bürger aber Kenntnis von solchen „Schattendateien" erhalten, stehen die Verantwortlichen unter Rechtfertigungszwang.

- Offene Bürotüren, herumliegende Unterlagen – „vorzugsweise" mit Sozial- und Steuerdaten –, unverschlossene bzw. nicht verschließbare Schränke usw. waren immer wieder festzustellen. Als die „organisatorische **Sicherheitslücke des Jahres**" konnte man ein Sozialamt bezeichnen, das im Erdgeschoß eines Ferienhauses untergebracht war. Damit die wartenden Antragsteller nicht in einem unbeleuchteten Flur stehen mußten, ließ man die Türen zu den Büroräumen geöffnet. So wußte nach einer halben Stunde Wartezeit jeder über jeden Bescheid und die Feriengäste, die den gleichen Flur nutzten, hatten am Ende ihres Urlaubs einen Gesamtüberblick.



Bei so eklatanten Sicherheitsmängeln hat natürlich keine der geprüften Stellen unseren Beanstandungen widersprochen. Es ist auch zu erwarten, daß man sich „bessert", aber – das ist die entscheidende Frage – warum erst, nachdem mit gehörigem Aufwand geprüft und beanstandet worden ist? Die zunehmende Zahl der positiven Beispiele zeigt, daß es auch anders geht. Warum für viele Kommunen so schwer zu realisieren ist, was für andere längst eine Selbstverständlichkeit ist, kann man kaum nachvollziehen. In der hergebrachten konventionellen Verwaltungswelt würde man sich über die festgestellten Mängel die Haare raufen. Für die Risiken der elektronischen Datenverarbeitung fehlt vielen offenbar die Sensibilität.

Was ist zu tun?
Unsere Prüfungsmaßnahmen werden unvermindert fortgeführt. Selbstverständlich sind aber die datenverarbeitenden Stellen gesetzlich verpflichtet, Mißstände gar nicht erst entstehen zu lassen. Die Kommunalparlamente sollten unsere Prüfberichte beraten, damit die Versäumnisse offenkundig werden.

4.1.3 Prüfung der Versorgungsausgleichskasse

Die Prüfung der Datenverarbeitung bei der Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein (VAK) ergab eine Reihe von Mängeln bei der Personalaktenführung und bezüglich der vertraulichen Behandlung der Beihilfedaten. Ihre Beseitigung packte die geprüfte Stelle mit hoher Priorität an.

Die VAK hat nach ihrer Satzung die Aufgabe, die Versorgungsbezüge der ehemaligen Bediensteten der Kommunen zu berechnen und auszuzahlen. Außerdem können die Kommunen die Beihilfen für ihre Bediensteten bei der VAK komplett bearbeiten lassen. Unsere Prüfung erstreckte sich auf die Beihilfebearbeitung, auf die Versorgung und auf die damit verbundene Umlageerhebung (Bereich Finanzdienstleistungen). Dabei wurden folgende Feststellungen getroffen.:

Fachbereich Beihilfekasse

- Beihilfeunterlagen für mehrere Arbeitnehmer wurden **in einer Akte** zusammengefaßt. Dies verstieß gegen die Regelung im Landesbeamtengesetz, wonach alle Unterlagen über einen Mitarbeiter in einer Beihilfeakte zusammenzuführen und von Vorgängen über andere Mitarbeiter getrennt zu führen sind.
- **Belege** (z. B. Heil- und Kostenpläne über Zahnbehandlungen, ärztliche Atteste zur Notwendigkeit von Aufwendungen usw.) wurden in den Beihilfeakten **gespeichert**, obwohl sie nach Abschluß der Bearbeitung mit dem Bescheid an die Betroffenen hätten zurückgegeben werden müssen.
- Beim Übergang der Beihilfebearbeitung auf die VAK wurden die bestehenden Unterlagen der Kommunen übernommen. Dabei waren die Daten aller Mitarbeiter einer Kommune **listenmäßig** zusammengestellt an die VAK übermittelt

worden. Diese hat dann seitenweise Kopien aus den Listen gefertigt und sie zu den jeweiligen Beihilfeakten genommen, ohne dabei die Daten der anderen Mitarbeiter unkenntlich zu machen. Die Speicherung von Beihilfedaten Dritter in den Beihilfeakten einzelner Mitarbeiter war ebenso zu beanstanden wie die Aufbewahrung der Unterlagen über die gesetzlich vorgeschriebene Speicherfrist von fünf Jahren hinaus.

- Für Beihilfeberechtigte, die in Pflegeheimen untergebracht waren, wurden **Bescheinigungen** über den Beihilfebezug ausgestellt und unmittelbar an die Krankenkassen übersandt, **ohne** daß dafür eine **Einwilligung** der Betroffenen vorlag. Ebenso wurden Auskünfte aus Beihilfevorgängen an behandelnde Ärzte ohne Einwilligung der Betroffenen erteilt.
- Das Verfahren der automatisierten Beihilfeabrechnung war nicht revisionsfähig dokumentiert. Ein **Sicherheitskonzept** fehlte ganz. Auch war die gesetzlich vorgeschriebene Erteilung von Auskünften an Betroffene über die zu ihrer Person gespeicherten Daten programmtechnisch nicht möglich.

Fachbereich Finanzdienstleistungen

- Für die Umlageerhebung zur Sicherung der Finanzierung von Versorgungsleistungen wurde für jeden Beamten eine sog. **Umlageakte** geführt. Sie enthielten auch Kopien aus den bei den Kommunen geführten Personalakten, obwohl diese Unterlagen zur Aufgabenerfüllung der VAK nicht erforderlich waren.
- Bei der **Aktenführung** wurde nicht zwischen Personalakten der Betroffenen und Umlageakten differenziert. Unterlagen zur Umlageberechnung und dienstrechtliche Entscheidungen gegenüber den Betroffenen wurden gemeinsam in einer Akte abgelegt. Dies entsprach nicht den Vorschriften über den Inhalt von Personalakten.
- Bei der Aufbewahrung von Umlageakten ausgeschiedener Beamter wurden die **Löschungsvorschriften** nicht beachtet.

Fachbereich Versorgung

- Bei der Versetzung von Beamten in den Ruhestand wurde zur Prüfung der Dienstunfähigkeit neben der eigentlichen Begutachtung vom **Amtsarzt** auch eine dienstrechtliche Bewertung des festgestellten Gesundheitszustandes verlangt. Diese Datenerhebung war nach den Bestimmungen des Landesbeamtengesetzes nicht zulässig.
- Nach Eintritt eines Versorgungsfalles wurden die Umlageakten als Versorgungsakten und damit als **Personalteilakten** weitergeführt, ohne vorher die Unterlagen zu entfernen, die nicht mehr benötigt wurden.
- Die **Kommunen** wurden über die Höhe der berechneten Versorgungsbezüge unterrichtet. Auch dies war nicht erforderlich und damit unzulässig.

Die VAK hat in ihrer Stellungnahme die dargestellten Mängel eingeräumt. Am Schluß der Stellungnahme kommt sie zu folgendem Ergebnis: „Die VAK wird die Vorgaben des Datenschutzbeauftragten hinsichtlich der Art und Weise der Aktenführung beachten und die bisherige Praxis umstellen. Der Aktenbestand wird, sofern es noch nicht geschehen ist, in angemessener Zeit neu geordnet werden. Nicht notwendige Belege und Unterlagen werden vernichtet bzw. zurückgesandt. Die einzelnen Verfahren werden in notwendiger und gebotener Weise dokumentiert werden."

Was ist zu tun?
Die Kommunen sollten künftig der VAK nur solche Daten bzw. Unterlagen übermitteln, die dort erforderlich sind.

4.1.4 Verwaltungsvorschriften zur Aufstellung von Bauleitplänen verbessert

Die Vorschriften des Baugesetzbuches sehen für die Aufstellung von Bebauungsplänen ein öffentliches Verfahren vor. Dies erfordert jedoch nicht zwangsläufig die namentliche Benennung der Einwender bei der öffentlichen Behandlung von Anregungen und Bedenken .

Wenn natürliche Personen **Einwendungen** gegen eine Bauleitplanung vortragen, sollten nach einem Runderlaß des Innenministers ihre Anschriften – sofern nicht besondere Vertraulichkeitsgründe vorliegen – **in öffentlicher Sitzung** genannt werden. Erst aus der Anschrift lasse sich die Belegenheit zum Plangebiet und damit das Maß der Betroffenheit erkennen.

Im Baugesetzbuch ist jedoch eine öffentliche Beratung von Anregungen und Bedenken in personenbezogener Form nicht zwingend vorgeschrieben. Auch erteilen die Betroffenen mit ihren Einwendungen weder durch schlüssiges Handeln noch durch ausdrückliche Erklärung ihre Einwilligung zur öffentlichen Beratung ihres Vorbringens.

Vielmehr ist die **Rechtsprechung** zu Planfeststellungsbeschlüssen (vgl. Tz. 4.6.3) auf die Bauleitplanung übertragbar. Danach ist es für die ordnungsgemäße Durchführung dieser Verfahren **nicht erforderlich**, die sachbezogenen Erwägungen zur Beurteilung und Gewichtung der geltend gemachten Einwendungen personenbezogen zu **veröffentlichen**. Unter dem Gesichtspunkt des Rechtsschutzes Betroffener reicht es aus, jedem Einwender eine Nummer zuzuordnen, ihm diese mitzuteilen und die Beratungen und Entscheidungen über die Einwendungen dann nur noch unter Angabe der Nummer durchzuführen. Auf diese Weise ist eine ausreichende Beratung der Anregungen und Bedenken bei der Bauleitplanung in öffentlicher Sitzung möglich. Es bestehen keine Bedenken dagegen, wenn den Mandatsträgern, soweit im Einzelfall erforderlich, eine entsprechende Referenzliste zur Verfügung gestellt wird.



Der Innenminister hat unsere Hinweise aufgegriffen. Nach einem neuen Erlaß sollen die Namen der Personen, die Anregungen vorgebracht haben, in öffentlicher Sitzung nicht mehr genannt werden.

4.2 Polizeibereich

4.2.1 Überblick

Auch 1998 wurden die Befugnisse der Polizei erneut erweitert. Anfang des Jahres wurde durch das „Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität" der **Große Lauschangriff** eingeführt. Damit verliert der Bürger seine letzte räumliche Rückzugsmöglichkeit vor staatlicher Überwachung. Bereits im letzten Jahr (20. TB, Tz. 2.2) hatten wir ausführlich unsere Argumente dargelegt, die wir im Gesetzgebungsverfahren gegen den Großen Lauschangriff vorgebracht hatten. Immerhin ist es aufgrund der von uns unterstützten öffentlichen Proteste gelungen, eine Ausnahme für die aus beruflichen Gründen zeugnisverweigerungsberechtigten Personen durchzusetzen. So dürfen Gespräche von Geistlichen, Ärzten, Anwälten, Journalisten, Abgeordneten, Drogen- oder Schwangerschaftsberatern auch in Wohnungen Dritter nicht überwacht werden. Auf der Strecke geblieben ist jedoch die Intimsphäre der Familie, für die offenbar keine ausreichende Lobby gegenüber den Strafverfolgungsinteressen mobilisiert werden konnte.

Derzeit wird die Umsetzung der durch Artikel 13 Grundgesetz festgeschriebenen Berichtspflichten der Sicherheitsbehörden über durchgeführte Lauschangriffe vorbereitet. Der Schleswig-Holsteinische Landtag muß ausreichende Informationen über das tatsächliche Ausmaß der Grundrechtsbeeinträchtigungen bei allen überwachten Personenkreisen erhalten. Er muß seine **parlamentarische Kontrolle** so wahrnehmen können, daß eine öffentliche Erörterung der Auswirkungen dieses weitreichenden Eingriffsinstruments möglich ist. Die nichtöffentlich tagende Parlamentarische Kontrollkommission ist dafür nicht geeignet.

Neue, datenschutzrechtlich sensible Fragen wirft der Aufbau einer präventiven Datei „genetischer Fingerabdrücke" beim Bundeskriminalamt, die **DNA-Analyse-Datei**, auf (vgl. Tz. 4.2.4). Gegen die offensichtlich erfolgversprechende Nutzung der Genomanalyse zum Tatnachweis – oder zur Entlastung – bei der Aufklärung von Straftaten ist aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Allerdings hätte das DNA-Identitätsfeststellungsgesetz an einigen Stellen präziser und enger gefaßt werden müssen. Seine Umsetzung durch das Bundeskriminalamt und in einigen Ländern läßt darüber hinaus befürchten, daß selbst diese Regelungen in der Praxis z. B. durch Einwilligungslösungen umgangen werden und es entgegen rechtsstaatlichen Garantien zu ungewollten Selbstbelastungen „freiwilliger" Probanden kommt.

Die polizeiliche Datenverarbeitungslandschaft steht bundesweit vor einer entscheidenden Neustrukturierung, die sich in dem Projekt **INPOL-neu** (Tz. 4.2.2) kristallisiert und Auswirkungen auf die gesamte polizeiliche Datenhaltung auch in den Ländern haben wird. Es geht im Grunde um die Ersetzung der einzelnen zu unterschiedlichen Zwecken angelegten polizeilichen Datensammlungen durch ein einheitliches Data-Warehouse-System. Damit droht das Wort Zweckbindung im Polizeibereich weitgehend zum Fremdwort zu werden.

Die bei einigen Polizeidienststellen durchgeführten **Kontrollen** erbrachten vereinzelte, aber keine gravierenden systematischen Mängel (vgl. Tz. 4.2.6). Offenbar zahlt sich langsam aus, daß die Polizei mit eigenen behördlichen Datenschutzbeauftragten viele Mängel von alleine bereinigt.

4.2.2 INPOL-neu

An der Neugestaltung des polizeilichen Informationssystems INPOL wird seit Jahren gearbeitet. Die Aufnahme des Echtbetriebes von „INPOL-neu" ist schon für das Jahr 2000 geplant. Die entscheidenden Weichenstellungen stehen jedoch noch aus. Der Beratung der datenschutzrelevanten Aspekte dieses Großprojekts kommt für das nächste Jahr deshalb eine besondere Bedeutung zu.

Kerngedanke von INPOL-neu ist das **„Data-Warehousing"** (vgl. Tz. 7.3). Zu jeder gespeicherten Person soll in einem einheitlichen Datenpool nur **ein Personendatensatz** bestehen, über den sämtliche auf sie bezogenen Sachverhalte erschlossen werden. Der Informationsumfang und die Recherchemöglichkeiten werden durch neue Funktionen wie „Gesamtauskunft" und „Fallkurzauskunft" sowie durch den umfassenden einheitlichen Fallbereich stark erweitert.

Dabei müssen aus unserer Sicht folgende Anforderungen beachtet werden:

- Es dürfen nur solche Sachverhalte an das Bundeskriminalamt übermittelt werden, die entsprechend dem Bundeskriminalamtgesetz (BKAG) **länderübergreifende oder erhebliche Bedeutung** haben. Personenbezogene Informationen, die diese Kriterien nicht erfüllen, dürfen nicht „vorsorglich" bundesweit zur Verfügung gestellt werden. Auch bei den sogenannten Meldediensten ist diese Relevanzschwelle zu beachten.
- Die einzelnen Nutzer dürfen nur zum **Zugriff** auf solche Daten berechtigt werden, die sie für ihren Aufgabenbereich brauchen. Insbesondere bei – noch ungesicherten – „weichen" Daten ist der Kreis der Zugriffsberechtigten zu begrenzen.
- Die **Errichtungsanordnungen** für die „logischen Dateien" müssen nach den Erfordernissen des jeweiligen Deliktsbereichs angemessen differenziert sein und dürfen nicht ein größtmögliches, deliktsneutrales Datenprofil erlauben.
- Das BKAG und noch mehr das schleswig-holsteinische Polizeirecht lassen eine Speicherung der Daten von **Opfern** und **Geschädigten** nur in sehr eingeschränktem Rahmen und grundsätzlich nur mit deren Einwilligung zu. Das Datenfeld „Geschädigter" darf also nicht routinemäßig geführt werden.
- Die **Abrufe** aus INPOL-neu sind vollständig zu **protokollieren**, damit neben der Mißbrauchsprävention auch im nachhinein eine wirksame Datenschutzkontrolle möglich ist. Die Nutzung von Protokolldaten zu polizeilichen Zwecken muß besonders genehmigt, dokumentiert und dem zuständigen Datenschutzbeauftragten mitgeteilt werden.

- Für das künftige technische System der Polizei muß ein hoher technischer **Sicherheitsstandard**, einschließlich der Verschlüsselung bei der Datenübertragung, selbstverständlich sein.

Die Landespolizei hat sich mit anderen Bundesländern zu einer Arbeitsgruppe zusammengeschlossen, um die technischen Voraussetzungen der Umsetzung von INPOL-neu auf Landesebene vorzubereiten. Wir sind beratend tätig.

Was ist zu tun?
Die Landespolizei muß INPOL-neu, z. B. bei der Vergabe von Nutzerberechtigungen, in datenschutzgerechter Weise umsetzen und beim Anschluß der Landessysteme an die INPOL-Bund-Schnittstelle einen hohen Sicherheitsstandard realisieren.

4.2.3 Landespolizeirecht oder Bundeskriminalamtgesetz

Die Auffassung, wonach für die Einstellung und Pflege von Daten in INPOL-Verbunddateien ausschließlich das Bundeskriminalamtgesetz (BKAG) gelte, verfestigt sich bei den Innenressorts immer mehr.

Wir haben über die Besorgnis, daß das Landespolizeirecht einem schleichenden Erosionsprozeß ausgesetzt wird, bereits vor Verabschiedung des neu gefaßten BKAG berichtet (vgl. 19. TB, Tz. 4.2.3). Auch der Wissenschaftliche Dienst des Landtages hat in einem Gutachten unsere Position geteilt. Der Innenminister hält jedoch bis heute an seiner Auffassung fest und argumentiert, INPOL könne sich nicht am „kleinsten gemeinsamen Nenner" der Landesgesetzgebung orientieren. Wir verstehen dagegen das föderale Kompetenzgefüge im Polizeirecht weiterhin so, daß für schleswig-holsteinische Datensätze in INPOL das schleswig-holsteinische **Landesrecht** als **Mindestschutzrahmen** für den Betroffenen gelten muß. Dies gilt gleichermaßen, wenn Daten an den bundesweiten Informationsverbund oder an EUROPOL übermittelt werden.

Konkret bedeutet dies z. B., daß in INPOL nach den Vorgaben des Landesverwaltungsgesetzes, anders als nach dem BKAG,

- vorbeugende Datenspeicherungen über Beschuldigte eine Einzelfallprognose voraussetzen,
- Opfer nur bei Gefahr besonders schwerer Taten mit kurzer Prüffrist abrufbar gespeichert werden dürfen,
- eine Prüffrist von im Regelfall fünf Jahren gilt.

Der Innenminister kann sich – ausgerechnet zu einer Zeit, in der wegen des Aufbaus weit in die Persönlichkeitssphäre hineingreifender EUROPOL-Dateien eine selbstbewußte Positionsbestimmung der Länder nötig ist – nicht über die Neu-

organisation der polizeilichen Datenlandschaft von dem vergleichsweise liberalen schleswig-holsteinischen Polizeirecht verabschieden. Es kann nicht angehen, daß personenbezogene Daten zwar nicht auf Landesebene, wohl aber auf Bundes- oder gar Europaebene gespeichert werden dürfen.

Was ist zu tun?
Das Land sollte seine gesetzgeberischen Kompetenzen verteidigen und das Landespolizeirecht nicht aushöhlen lassen.

4.2.4 Genetischer Fingerabdruck

Der Gesetzgeber hat eine gesetzliche Grundlage für die Erhebung und Speicherung sog. genetischer Fingerabdrücke für die Zwecke künftiger Strafverfahren geschaffen. Auch wenn grundsätzlich einleuchtet, daß Polizei und Justiz die modernen Techniken der DNA-Analyse für die Strafverfolgung nutzen dürfen, muß hier ein hoher Standard für den Persönlichkeitsschutz gelten. Die bundesweiten Ausführungsbestimmungen werden diesem Anspruch noch nicht gerecht.

Im September 1998 ist das **DNA-Identitätsfeststellungsgesetz** in Kraft getreten. Danach können bei Beschuldigten und Verurteilten die zu ihrer künftigen Identifizierung in Strafverfahren notwendigen genetischen Informationen erhoben, untersucht und beim BKA gespeichert werden. Dies betrifft zwar lediglich die Informationen des sogenannten nicht-codierenden Bereiches der DNA, die nach heutigem Stand der Wissenschaft noch keine Rückschlüsse auf Persönlichkeitsmerkmale oder andere individuelle genetische Dispositionen erlauben. Aufgrund der rasanten Entwicklung – weltweit wird an der vollständigen Entschlüsselung des menschlichen Genoms gearbeitet – kann aber nicht ausgeschlossen werden, daß künftig auch aus diesen Merkmalen sensible Erbinformationen ableitbar sind. Deshalb darf der genetische Fingerabdruck dem herkömmlichen, daktyloskopisch auszuwertenden Fingerabdruck nicht gleichgesetzt werden. Es bedarf hier strengerer datenschutzrechtlicher Absicherungen.

Die Regelungen im DNA-Identitätsfeststellungsgesetz genügen diesem Anspruch nicht:

- Der Katalog von Straftaten, bei denen eine DNA-Analyse zur präventiven Speicherung angeordnet werden darf, umfaßt neben Verbrechen und Sexualdelikten u. a. auch Banden- und Einbruchsdiebstähle. Die zusätzliche Öffnungsklausel in Richtung der sonstigen **„Straftaten von erheblicher Bedeutung"** erscheint sachlich nicht gerechtfertigt und ist zu unbestimmt.
- Eine **nachträgliche Datenerhebung** bei Personen, die bereits verurteilt wurden und ihre Strafe möglicherweise bereits abgesessen haben, ist ausdrücklich vorgesehen. Aus Verhältnismäßigkeitsgründen wäre bei Verurteilten jedoch eine Einschränkung des Deliktskatalogs z. B. auf Verbrechen, Sexual- und Körperverletzungsdelikte angebracht gewesen.

- Der Gesetzgeber hat lediglich auf die allgemeinen **Speicherungs- und Verwendungsregelungen** im BKAG verwiesen. Hintergrund war eine bereits vor Verabschiedung des Gesetzes vom BKA erlassene Errichtungsanordnung für die DNA-Analyse-Datei, die so durch den Gesetzgeber im wesentlichen „abgesegnet" wurde. Aus unserer Sicht müßte die Nutzung der DNA-Daten durch das BKA und die Übermittlung an andere Behörden auf die Verfolgung oder Verhütung von Straftaten nach dem Katalog des DNA-Identitätsfeststellungsgesetzes begrenzt werden.
- Außerdem fehlt eine gesetzliche Regelung zum Umgang mit **„freiwillig" abgegebenen DNA-Proben**. Diese dürften nicht einfach mit den in der DNA-Datei gespeicherten Spuren aus anderen unaufgeklärten Taten abgeglichen werden oder gar selbst zu einer Speicherung in der Datei führen. Geklärt werden müßte vom Gesetzgeber auch, unter welchen Umständen die Untersuchungsergebnisse aus „freiwilligen" Proben zur Belastung eines Verwandten eines Probanden, der sich auf sein Zeugnisverweigerungsrecht beruft, genutzt werden dürfen.

Mittlerweile liegt zur **Errichtungsanordnung des BKA** ein überarbeiteter Entwurf vor. Vorgesehen ist darin entgegen den gesetzlichen Vorgaben:

- eine präventive Speicherung von DNA-Profilen, die zur Beweisführung in einem Strafverfahren erstellt wurden, ohne daß ein Richter die Prognose möglicher erneuter Begehung schwerer Taten bejaht hat;
- die Speicherung von DNA-Profilen allein auf Grundlage einer „Einwilligung", also unter Umgehung des richterlichen Entscheidungsvorbehalts, sowie
- Anfragen an die DNA-Analyse-Datei mit den Personalien einer Person, obwohl allein die Anfrage mit DNA-Identifizierungsmustern dem Zweck der Datei entspricht.

Nach einem Erlaß des Justizministeriums werden bei der gerade angelaufenen Erfassung der genetischen Fingerabdrücke von Gefangenen in schleswig-holsteinischen Justizvollzugsanstalten DNA-Analysen, anders als offenbar in anderen Bundesländern, nicht auf „freiwilliger" Grundlage, sondern nur auf richterliche Anordnung hin durchgeführt. Auch eine Übermittlung aus Strafverfahren vorhandener DNA-Analyse-Daten an die Datei beim BKA setzt nach dem Erlaß eine richterliche Anordnung voraus.

Was ist zu tun?
Der Innenminister sollte sich dafür einsetzen, daß die Errichtungsanordnung des BKA für die DNA-Analyse-Datei den gesetzlichen Vorgaben angepaßt wird.

4.2.5 Schleierfahndung oder nicht?

Während anlaßfreie Personenkontrollen der Polizei nach dem Muster der in anderen Bundesländern eingeführten „Schleierfahndung" in Schleswig-Holstein keine parlamentarische Mehrheit gefunden haben, hat die Verkehrspolizei ein neuartiges Konzept zur Kriminalitätsbekämpfung auf Autobahnen auf der Grundlage von Lagebildern verwirklicht. Dieses stützt sich auf eine Rechtsgrundlage im Landesverwaltungsgesetz zur sog. Razzia an gefährlichen Orten. Hierbei darf allerdings die Grenze zur verdachtsunabhängigen Schleierfahndung nicht überschritten werden.

Im 19. Tätigkeitsbericht (Tz. 4.2.5) haben wir dargelegt, warum wir die gesetzliche Einführung der **Schleierfahndung** aus rechtsstaatlichen Gesichtspunkten und als Verstoß gegen den „Vertrag von Schengen", wonach gerade ein Abbau von Personenkontrollen stattzufinden hat, abgelehnt haben. An dem Grundsatz, daß ein polizei- oder strafrechtlich relevanter Anlaß bestehen muß, bevor die Polizei jemanden anhalten, durchsuchen oder seine Personalien mit polizeilichen Dateien abgleichen darf, muß sich deshalb auch das im Februar 1998 vorgestellte Konzept des Innenministers zur Einführung verstärkter **Autobahnkontrollen zur Kriminalitätsbekämpfung** messen lassen. Auf unsere Nachfrage erläuterte uns der Innenminister die wesentlichen Eckpunkte des Konzepts wie folgt:

- Rechtsgrundlage für die durchgeführten Kontrollen sei die Befugnis zur Identitätsfeststellung „an einem Ort, an dem zu diesem Zeitpunkt Tatsachen für die Verabredung, Vorbereitung oder Verübung von Straftaten oder das Verbergen gesuchter Straftäter sprechen" (§ 181 Abs. 1 S. 2 Nr. 1 LVwG – **„Razzia"**). Ein Surrogat für weggefallene Grenzkontrollen sei – trotz des von der Verkehrspolizei verwendeten Begriffs der „Ausgleichsmaßnahmen" – nicht beabsichtigt.
- Die Kontrollen sollen als **Gefahrerforschungseingriff** nur bei sich häufenden Delikten stattfinden.
- Es dürfen bei einer solchen „Razzia" nur **auffällige Fahrzeuge** und **Personen** angehalten und überprüft werden.

Wir haben, um uns ein Bild von der tatsächlichen Verfahrensweise zu machen, an einer gemeinsamen stationären Autobahnkontrolle zur Kriminalitätsbekämpfung der Polizei, des Bundesgrenzschutzes und des Zolls teilgenommen. Ein datenschutzrechtlich relevantes Überschreiten der polizeirechtlichen Befugnisse der Polizei haben wir dabei nicht festgestellt.

Mit einer verkappten Schleierfahndung sind die „neuartigen Autobahnkontrollen" nach unserer derzeitigen Einschätzung nicht gleichzusetzen. Dennoch ist diese Form der von einer reinen Verkehrskontrolle abzugrenzenden lagebildabhängigen Kontrolle, gemessen an den gesetzlichen Anforderungen an eine „Razzia" nach LVwG, für die Polizei eine **Gratwanderung zur Jedermannkontrolle**: Das zugrundeliegende Lagebild muß so aussagekräftig sein, daß die kontrollierten Personen an dem betreffenden Ort und zur Zeit der Kontrolle hinreichenden Anlaß

für einen Gefahrerforschungseingriff bieten. Es müssen zudem die gesonderten Rechtsgrundlagen für Datenabgleiche, Durchsuchungen oder weitere Maßnahmen gegenüber jedem betroffenen Fahrzeuginsassen beachtet werden. Wenn dies der Fall ist, kann gegen eine Nutzung der verkehrspolizeilichen Ressourcen für die Bekämpfung von Kriminalität aus unserer Sicht nichts eingewandt werden.

Was ist zu tun?
Die Polizei muß bei den neuen Autobahnkontrollen zur Kriminalitätsbekämpfung in jedem Einzelfall sicherstellen, daß sich aus dem Lagebild ausreichende Anhaltspunkte für die Eingrenzung auf potentielle Störer und künftige Straftäter ableiten lassen.

4.2.6 Prüfungen bei Polizeistationen

„Angemeldete Unangemeldete Kontrollen" (AUK) bei einigen Polizeistationen ergaben einen recht guten Datenschutzstandard. Auf festgestellte Detailmängel reagierte die Polizei prompt.

Bei den Prüfungen im Bereich der Polizeidirektion Süd ging es schwerpunktmäßig um die Datensicherheit in den Polizeistationen (vgl. zur AUK Tz. 4.12). Wir haben aber auch **stichprobenweise** kontrolliert, ob für die personenbezogenen Unterlagen die Aufbewahrungsfristen eingehalten und ob mehr Daten als zulässig und erforderlich gespeichert wurden.

Dabei stießen wir auf **Defizite** der folgenden Art:

- Teilweise konnten Besucher im Wachraum den Polizeifunk, über den sensible personenbezogene Daten abgefragt und übermittelt werden, durch die dort aufgestellte Funksprechanlage mithören.
- In einigen Einsatzdokumentationen (Einsatzberichte, Vorgangsdurchschriften, Gewahrsamsbuch) fanden sich Ausdrucke aus Dateien wie PED und ZEVIS, deren Aufbewahrung über den Zeitpunkt der aktuellen Sachbearbeitung hinaus nicht erforderlich und auch nicht statthaft war, da auf diese Weise zwischenzeitliche Datenlöschungen unwirksam würden.
- In einem Gewahrsamsbuch befanden sich detaillierte medizinische Daten.
- In einer Station fanden wir „Übernachtungsbescheinigungen" für eine städtische Obdachlosenunterkunft. Sie mußten von den Betroffenen auf Veranlassung der Stadt vor der Aufnahme in die Unterkunft beigebracht werden. In ihnen bestätigte die Polizei nach Abgleich der Personalien mit der PED, keine Bedenken gegen eine Übernachtung der Person zu haben. Für dieses Verfahren gab es beim besten Willen keine Rechtsgrundlage!
- Einzelplatz-PC wurden ohne die erforderliche Dokumentation, Nachweis im Geräteverzeichnis, Verfahrensbeschreibung, Test und Freigabe der eingesetzten Verfahren genutzt.

Diese Mängel wurden von den betreffenden Dienststellen in Zusammenarbeit mit der Polizeidirektion umgehend behoben.

Was ist zu tun?
In allen Polizeidienststellen des Landes sollte geprüft werden, ob vergleichbare Mängel vorliegen. Gegebenenfalls sollten sie umgehend abgestellt werden.

4.2.7 ZEVIS-Abfrage mit schwerwiegenden Folgen?

Ein gezielter Mißbrauch der Daten von Kfz-Haltern aus ZEVIS zu privaten Zwecken ist bei der Polizei derzeit nicht in jedem Falle über die Protokollierung und Dokumentation von Abfragen aufklärbar. Ein Petent wurde möglicherweise Opfer eines solchen Mißbrauchs.

Bei einer Auseinandersetzung zwischen zwei Pkw-Fahrern hatte sich einer der beiden demonstrativ die Kfz-Nummer des anderen aufgeschrieben und Konsequenzen angedroht. Kurz darauf wurden am Fahrzeug des Petenten vor seiner Wohnung die Reifen zerstochen und der Lack mit Säure zerstört. Seine Familie war wochenlang Drohanrufen ausgesetzt. Eine Überprüfung ergab, daß in der Zeit zwischen dem Vorfall und der Beschädigung bzw. dem Beginn der Drohanrufe die Personalien und Anschrift des Petenten über eine **Kfz-Halterabfrage** an das Kraftfahrt-Bundesamt von der Datenstation einer Polizeidirektion telefonisch an ein Polizeirevier übermittelt worden waren.

Wozu die Abfrage erfolgte, ließ sich aufgrund von **Erinnerungslücken** des anfragenden Beamten und fehlender schriftlicher Aufzeichnungen bei seiner Dienststelle nicht mehr klären. Die Polizei räumte ein, es sei nach dem praktizierten Verfahren nicht ausgeschlossen, daß ein unbefugter Kollege die telefonische Anfrage an die Datenstation unter dem Namen eines Polizeibeamten vorgenommen hat. Demzufolge war es bislang weder möglich, dem in der technischen Protokollierung erfaßten Beamten einen eklatanten Datenmißbrauch nachzuweisen, noch ihn vollständig von einem dahin gehenden Verdacht zu entlasten. Ein staatsanwaltliches Ermittlungsverfahren wurde eingestellt.

Nach den Vorschriften des Straßenverkehrsgesetzes und der Fahrzeugregisterverordnung findet im Kraftfahrt-Bundesamt und bei der Datenzentrale eine automatische Protokollierung sämtlicher Abrufe aus dem Zentralen Verkehrsinformationssystem (ZEVIS) statt. Trotzdem stehen der gesetzlich geforderten Möglichkeit einer nachträglichen Rechtmäßigkeitsprüfung folgende **Dokumentationslücken** entgegen:

- Bei telefonischen Anfragen wird die **Identität** des Anfragenden nicht überprüft; nur bei Zweifeln erfolgt ein Rückruf. Es ist also möglich, durch falsche Namensnennung Spuren zu verwischen und unter Umständen Polizeibeamte erheblich zu belasten. Das Mißbrauchsrisiko könnte nach unserer Auffassung zumindest gesenkt werden, wenn bei der Datenstation zusätzlich die Dienstausweisnummer des Anrufenden registriert würde.

- Es wird nicht in allen Bereichen der polizeilichen Sachbearbeitung verlangt, daß zu einer Anfrage an ZEVIS ein schriftlicher Vorgangsnachweis in der Form einer Tätigkeitsbucheintragung existiert, über den sich im nachhinein feststellen läßt, ob ein berechtigter Grund für die Anfrage vorlag. Die fehlende Erinnerung des Beamten an einen konkreten Vorgang als Abfragegrund bedeutet ohne solchen Nachweis derzeit bereits das Ende der Fahnenstange einer datenschutzrechtlichen Kontrolle. Deshalb unsere Forderung: keine Anfrage aus Polizeidienststellen ohne zugrundeliegenden **Vorgangsnachweis**! Ausnahmen sollten allerdings für besondere Tätigkeitsbereiche – z. B. Kontrollen auf der Straße – gelten, wo schriftliche Nachweise nicht immer geführt werden können.

Unsere Beanstandung im Falle des Petenten will die Polizei aber nicht zum Anlaß nehmen, unsere praktikablen Vorschläge zur Verbesserung des Verfahrens umzusetzen. Er hält die derzeitige Protokollierung für ausreichend. Ein Ergebnis, das wir dem Betroffenen nicht verständlich machen konnten.

Was ist zu tun?
Der Innenminister muß Konsequenzen aus diesem Fall ziehen und durch geeignete Verfahrensvorkehrungen seine datenschutzrechtliche Verpflichtung umsetzen, eine zweifelsfreie Nachvollziehbarkeit der Rechtmäßigkeit von ZEVIS-Abfragen zu gewährleisten.

4.2.8 Evaluierung polizeilicher Befugnisse – Verwaltungsfachhochschule Altenholz startet ein Untersuchungsprojekt

Bereits vor einigen Jahren hat das Innenministerium zugesagt, die Erforderlichkeit und Wirksamkeit polizeilicher Eingriffsbefugnisse einer objektiven Evaluierung zu unterziehen. Dies ist aber aus Haushaltsgründen nicht erfolgt. Nun wird ein entsprechendes Projekt durch die Verwaltungsfachhochschule in Altenholz realisiert.

Das Innenministerium hat nunmehr bei der Verwaltungsfachhochschule ein **Gutachten** in Auftrag gegeben, das in einem repräsentativen Umfang abgeschlossene Strafverfahren, in denen besonders tiefgehende Eingriffsbefugnisse durch Polizei und Staatsanwaltschaft angewandt wurden, untersuchen soll (vgl. 19. TB, Tz. 10.4). Analysiert werden soll z. B.

- der Umfang von Telefonüberwachungen und die Anfertigung von Bild- und Tonaufnahmen im Hinblick auf die Anzahl der in ihren Grundrechten betroffenen Personen, die Dauer des Eingriffs sowie die betroffenen Räumlichkeiten (Privatwohnungen oder Geschäftsräume),
- die hierdurch gewonnenen beweisrelevanten Ergebnisse und
- die denkbaren alternativen Vorgehensweisen.

Es sollen aber auch Aussagen darüber getroffen werden, ob die vorhandenen Rechtsgrundlagen der Polizei sinnvolle Handlungsmöglichkeiten bieten oder ob sie den Ermittlungserfolg im Einzelfall gemindert haben.

Sinn und Absicht des Projekts ist es nicht, die oft mühevolle Arbeit von Ermittlern in den jeweils untersuchten Strafverfahren im nachhinein „auseinanderzunehmen". Vielmehr soll eine **fundierte Aussage** zur Frage erarbeitet werden, wie sich das in den letzten Jahren stark angewachsene **Instrumentarium der Polizei** in der Praxis auf die Grundrechte von Beschuldigten und dritten Personen auswirkt. Diese Fragestellung unterscheidet das schleswig-holsteinische Projekt von der Rechtstatsachensammelstelle des BKA. In der Konsequenz der Untersuchung sollten Befugnisse, die sich nicht bewährt haben, gegebenenfalls wieder gestrichen werden. An der Durchführung des Projektes werden wir seitens des Innenministeriums beteiligt. Man bemüht sich auch um eine Kooperation mit anderen Bundesländern, um zu repräsentativeren Aussagen zu gelangen. Erste Ergebnisse sollen Ende 1999 vorliegen.

Was ist zu tun?
Justiz und Polizei sollten das Vorhaben durch das Bereitstellen der erforderlichen Informationen unterstützen.

4.2.9 Polizeifunk für alle?

Bei der Schaffung eines allgemeinen Informationszugangsrechts ist die Polizei anderen staatlichen Stellen mehr oder weniger freiwillig einige Schritte voraus. Das Abhören des Polizeifunks ist mittlerweile ohne Kosten und Mühen für jedermann möglich und erfreut sich offenbar größter Beliebtheit. Mit Bestrafung muß man kaum rechnen.

Seit jeher stellt es für **ehrgeizige Funkamateure** eine echte Herausforderung dar, Geräte zu bauen, mit denen sich der Polizeifunk und anderer behördlicher Funkverkehr abhören läßt. Zu dem erforderlichen technischen Wissen kam aber bislang das Risiko der Strafbarkeit. Bereits der Beginn des Zusammenbaus wurde als strafbarer Versuch angesehen, eine Fernmeldeanlage zu errichten. Verkäufer solcher Geräte mußten damit rechnen, daß Polizeibehörden zur Abwehr von Gefahren die Geräte sicherstellten und einzogen.

Im Jahr 1992 kam es dann allerdings durch eine Vorgabe der EG zu einer Aufweichung der Rechtsvorschriften. Danach war der Besitz der Abhörgeräte nicht mehr strafbar. Die fortschreitende Computertechnik tat ein übriges. Heute sind sogenannte **Scanner**, mit denen sich der Funkverkehr der Polizei, der Rettungsdienste und anderer Stellen aufspüren läßt, bereits für ca. 40 DM erhältlich. Es gibt umfangreiche Spezialliteratur inklusive regelmäßig erscheinender Zeitschriften zu dem Thema; der Handel hält sogar CD-ROMs bereit, die die Frequenzbänder des Funkverkehrs unterschiedlicher Behörden, z. B. der Polizeidienststellen verschiedener Städte, nachweisen.

Wir haben bereits im 15. Tätigkeitsbericht (Tz. 6.2.4) und im 16. Tätigkeitsbericht (Tz. 4.3.5) auf die damit verbundenen Gefahren aufmerksam gemacht und verlangt, daß die Polizeibehörden ihren **Funkverkehr** in **verschlüsselter Form** abwickeln. Wenn schon erstaunlicherweise kein operatives Problem darin gesehen wird, daß fast der gesamte Funkverkehr der Polizei abgehört wird und dadurch z. B. Pressevertreter häufig vor der Polizei am Einsatzort eintreffen, ist jedenfalls zur Wahrung des informationellen Selbstbestimmungsrechts die Abschottung der behördlichen Kommunikation vor privater Neugier geboten. Die Ausführungen im 16. Tätigkeitsbericht haben weiterhin Gültigkeit: „Für Polizei und Rettungspersonal ist die Beschäftigung mit Menschen und Personalien alltägliche Praxis. Mit Hilfe des Funkgerätes wird überprüft und berichtet, z. B. wer Halter eines Fahrzeugs ist, ob jemand gesucht wird, wo ein Betroffener wohnt und vieles andere mehr. So wandern zwangsläufig brisante Informationen zumindest in Auszügen durch den Äther. Vom Einsatzort wird gemeldet, was mit Betroffenen geschehen ist (z. B. Festnahme, Blutprobe, Anzeige, Einlieferung in das Krankenhaus mit Diagnose), welcher Ehestreit zu schlichten war, wer wen geschlagen hat usw." Bei unverschlüsselter Übermittlung kann ein Betroffener fast sicher sein, daß er z. B. bei einer routinemäßigen Verkehrskontrolle, bei der seine Halterdaten über Funk mit dem Register abgeglichen werden, zur Unterhaltung einiger „Funkamateure" beiträgt.

Bis vor kurzem konnte der Gesetzgeber noch darauf verweisen, daß das **Telekommunikationsgesetz** eine Vorschrift enthält, durch die das unerlaubte Abhören des Funkverkehrs unter Strafe gestellt wird. Nach § 86 Satz 1 TKG dürfen nämlich mit einer Funkanlage solche Nachrichten nicht abgehört werden, die für die Funkanlage nicht bestimmt sind. Allerdings haben zwei strafgerichtliche Entscheidungen aus jüngerer Zeit gezeigt, daß die Vorschrift im wesentlichen leerläuft. Nach dieser Rechtsprechung muß nämlich der Täter auf frischer Tat angetroffen werden. Außerdem muß dem benutzten Gerät anzusehen sein, daß es nicht zum Abhören bestimmter Funkverkehre eingesetzt werden darf.

Polizei wie Bürger müssen also offenbar weiter damit leben, daß die Übertragung von personenbezogenen Daten über den **Polizeifunk quasi öffentlich** stattfindet. Erst für die Zeit zwischen 2002 und 2008 ist bei der schleswig-holsteinischen Polizei die Einführung eines digitalen Funksystems geplant, bei dem dann auch die Möglichkeit der Verschlüsselung besteht. Die Verschlüsselung des zur Zeit eingesetzten analogen Funkverkehrs ist nach Aussage der Verantwortlichen zu teuer und zudem technisch relativ leicht zu überwinden. Diese Sorglosigkeit gerade der Sicherheitsbehörden überrascht, wird doch sonst bei vielen Gelegenheiten Klage über all das geführt, was der Polizei bei ihrem Kampf gegen das Verbrechen (vermeintlich oder tatsächlich) im Weg steht.

Was ist zu tun?
Die für die Ausrüstung der Polizei verantwortlichen Stellen sollten sich zum Schutz personenbezogener Daten und im Interesse der operativen Sicherheit endlich dazu durchringen, den polizeilichen Funkverkehr durch Verschlüsselungstechniken zu schützen. Außerdem muß geprüft werden, ob § 86 Telekommunikationsgesetz in seiner jetzigen Form als Strafvorschrift ausreicht.

4.3 Verfassungsschutz – Sicherheitsüberprüfungsgesetz läßt weiter auf sich warten

Von einem Bedeutungswandel des Geheimschutzes nach Wegfall der Ost-West-Konfrontation ist in einem Referentenentwurf des Innenministeriums für ein Sicherheitsüberprüfungsgesetz wenig zu spüren. Auch die Ergebnisse unserer Kontrollen bei behördlichen Geheimschutzbeauftragten im Jahr 1991 müssen endlich berücksichtigt werden. Schleswig-Holstein droht Schlußlicht bei der Gesetzgebung für Sicherheitsüberprüfungen zu werden.

Obwohl eine Sicherheitsüberprüfung einen empfindlichen staatlichen Eingriff in die Privatsphäre darstellt, werden derartige Überprüfungen in Schleswig-Holstein ohne Rechtsgrundlage durchgeführt (vgl. 20. TB, Tz. 4.3.2). Eine Reihe anderer Bundesländer hat dagegen Sicherheitsüberprüfungsgesetze verabschiedet, in denen das herkömmliche Überprüfungsverfahren, für das die politischen Gegebenheiten des Kalten Krieges kennzeichnend waren, verändert worden ist. Ausgangspunkt unserer Stellungnahme zu einem **Referentenentwurf** des Innenministeriums war deshalb, daß ein auf dem Grundsatz der Freiwilligkeit basierendes Verfahren nicht stärker in das Persönlichkeitsrecht eingreifen sollte als für den jeweiligen Überprüfungszweck erforderlich. Wichtig wäre zudem eine Reduzierung des Umfanges an Verschlußsachen und der in Frage kommenden Dienstposten, um das **Sicherheitsüberprüfungsverfahren** zu **verschlanken**. Im einzelnen haben wir folgende Änderungen vorgeschlagen:

- Die bislang in Schleswig-Holstein bestehende Einrichtung eines **Sicherheitsbeauftragten des Landes** sollte beibehalten und durch Kompetenzverlagerungen zu Lasten der behördlichen Geheimschutzbeauftragten gestärkt werden. Der Sicherheitsbeauftragte sollte zur Wahrung seiner fachlichen Unabhängigkeit organisatorisch aus der Verfassungsschutzbehörde herausgelöst werden. Würde er abgeschafft, wären bei jedem behördlichen Geheimschutzbeauftragten höchst sensible Sicherheitsakten über die in der Dienststelle beschäftigten überprüften Personen zu führen.
- Der **Betroffene** muß **unterrichtet** werden, wenn im Verlauf seiner Überprüfung weitergehende Maßnahmen erforderlich werden als durch seine Einwilligung in das Verfahren gedeckt sind. Die Gründe für eine Befragung von anderen Personen oder Stellen als zunächst vorgesehen müssen in der Sicherheitsakte dokumentiert werden.
- Mitbetroffene Personen, z. B. **Eltern** und **Partner** müssen aus dem Gesetz ersehen können, inwieweit über sie Informationen eingeholt und gespeichert werden dürfen. Dies betrifft insbesondere Abgleiche ihrer Daten mit dem Informationssystem NADIS der Verfassungsschutzbehörden.
- Im Wege der **Anhörung** muß der **Betroffene** zu Erkenntnissen aus der Befragung Dritter Stellung nehmen können, um sich gegen unberechtigte Vorbehalte wehren zu können. Gezielte unfaire „Anschwärzungen" sollten im Sicherheitsüberprüfungsverfahren keine Chance haben!

- Angaben zu möglichen Sicherheitsrisiken aufgrund von **psychischen** oder **gesundheitlichen Defiziten** des Betroffenen sollten nur dann Eingang in die Sicherheitsakte finden, wenn sie von fachlich qualifizierter Seite bestätigt worden sind.
- Die Rechte von Betroffenen auf **Auskunft und Akteneinsicht** sollten übersichtlich und für alle am Verfahren beteiligten Behörden einheitlich geregelt werden. Von der veralteten Vorstellung, eine Einsicht in Sicherheitsakten dürfe es grundsätzlich nicht geben, sollte Abschied genommen werden, da berechtigte Sicherheitsinteressen über Ausnahmeregelungen geschützt werden können.
- **Private Stellen**, bei denen Sicherheitsüberprüfte beschäftigt werden, dürfen nur Daten zum Verfahrensablauf speichern und müssen insoweit der Kontrolle des Landesdatenschutzbeauftragten unterliegen.
- Ausnahmen von den **Kontrollbefugnissen** des **Landesdatenschutzbeauftragten**, die es in Schleswig-Holstein auch im Verfassungsschutzbereich schon lange nicht mehr gibt, sollten nicht ausgerechnet bei Sicherheitsüberprüfungen eingeführt werden, gerade da, wo es um Informationen mit möglichen unmittelbaren beruflichen Auswirkungen für die hierbei Betroffenen geht!
- Da sämtliche Datenerhebungen auf der Grundlage einer **Einwilligung** des Betroffenen erfolgen, dürfen sie entgegen ihrer ursprünglichen Zweckbestimmung nur zur Verfolgung schwerster Straftaten genutzt werden. Auch die Befugnis der Verfassungsschutzbehörde, sich aus dem Fundus der Sicherheitsüberprüfungsdaten „selbst zu bedienen", sollte auf die Aufklärung von Bestrebungen im Terrorismus-, Spionage- bzw. gewaltgeneigten Extremismusbereich beschränkt bleiben.

Zu unserer Stellungnahme hat sich der Innenminister bislang noch nicht geäußert. Offenbar wird das Vorhaben derzeit nicht weiter vorangetrieben.

Was ist zu tun?
Der Innenminister sollte unter Berücksichtigung unserer datenschutzrechtlichen Anregungen das Gesetzgebungsverfahren endlich in Gang setzen, damit noch in dieser Legislaturperiode eine Rechtsgrundlage für Sicherheitsüberprüfungen verabschiedet werden kann.

4.4 Justizverwaltung

4.4.1 Überblick

Für Mitteilungen der Justiz an Dritte sowie für den Strafvollzug hat der Bundesgesetzgeber in den letzten beiden Jahren im **Justizmitteilungsgesetz** und im **Strafvollzugsgesetz** (vgl. Tz. 4.4.2 sowie 9.5) endlich bereichsspezifische Rechtsgrundlagen für den Datenschutz geschaffen. Die grundlegenden Regelungen für die Verarbeitung personenbezogener Daten im Strafverfahren stehen dagegen nach wie vor aus. Dabei besteht in Schleswig-Holstein die Besonderheit, daß die Datenverarbeitung in dem mittlerweile bei allen Staatsanwaltschaften eingeführten System MESTA (früher GAST) durch bereichsspezifische, landesrechtliche Regelungen abgedeckt ist.

Die Arbeiten zur Einführung der beiden großen **Automatisierungsvorhaben** (MESTA bei den Staatsanwaltschaften, MEGA bei den Amtsgerichten (vgl. Tz. 4.4.3)) sind im wesentlichen abgeschlossen. Als neues Großprojekt steht nun die Einführung des elektronischen Grundbuches (EGB, vgl. Tz. 5.1) bevor.

Auffallend war im Berichtsjahr ein **Anstieg von Eingaben** zu den Themenbereichen „Einsichtnahme in das Grundbuch" und „Schuldnerverzeichnis" (vgl. Tz. 4.4.4). Auch wenn unsere Nachprüfungen nur in wenigen Fällen ein datenschutzrechtliches Fehlverhalten der betroffenen Stellen ergaben, zeigte sich doch, wie bedeutsam eine vorschriftsgemäße Handhabung dieser sensiblen Daten insbesondere für die berufliche Situation des einzelnen ist und wie schwer es sein kann, zu Unrecht gespeicherte und übermittelte Daten wieder „einzufangen".

4.4.2 Datenschutzregelungen für den Strafvollzug

Der Bund hat mit dem 4. Strafvollzugsänderungsgesetz bereichsspezifische Datenschutznormen für den Strafvollzug eingeführt. Leider sind die neuen Datenverarbeitungsbefugnisse, insbesondere durch Initiativen des Bundesrats, in einigen Punkten viel zu weitgehend.

Daten über den Strafvollzug gehören auch nach der EU-Datenschutzrichtlinie zur Kategorie der **besonders sensiblen Informationen**. Durch strenge Verarbeitungsregelungen muß gewährleistet sein, daß sie nicht in falsche Hände geraten. Dem wird das neue Strafvollzugsgesetz wegen zu weiter Generalklauseln nicht gerecht.

Als Beispiele für bedenklich **konturenlose Datenverarbeitungsbestimmungen** sind zu nennen:

- Daten aus dem Strafvollzug können für vollzugsfremde Zwecke an öffentliche Stellen übermittelt werden, wenn dies durch anderweitige, teilweise unbestimmte gesetzliche Vorschriften vorgesehen ist.
- Durch eine dehnbare Generalklausel wird auch die Erhebung von Daten über dritte Personen (Verwandte, „Urlaubsadressen", Besucher) erlaubt.

- Die besondere Schweigepflicht der Ärzte, Psychologen und Sozialarbeiter ist weitgehend aufgehoben; sie müssen Daten, die ihnen Gefangene anvertraut haben, gegenüber dem Anstaltsleiter dann bereits offenbaren, wenn es der „Aufgabenerfüllung der Vollzugsbehörde dient".
- Akteneinsicht in die über sie geführten Unterlagen erhalten Gefangene lediglich zur Wahrnehmung rechtlicher Interessen. Außerdem werden sie zunächst auf die Auskunft verwiesen.
- Auch nach der Entlassung dürfen Lichtbild und Personenbeschreibung des Gefangenen weiter aufbewahrt werden, obwohl es hierfür weder eine vollzugliche noch eine polizeiliche Notwendigkeit gibt. Wir hatten zuvor bei einer Querschnittsprüfung erreicht, daß Gefangene die Vernichtung ihrer Lichtbilder nach Entlassung verlangen können.
- Schließlich sind die Fristen für die Aufbewahrung von Gefangenenpersonalakten, Gesundheitsakten und Gefangenenbüchern mit zwanzig bzw. dreißig Jahren außergewöhnlich lang geraten. Selbst diese Fristen können in bestimmten Fällen noch verlängert werden.

Was ist zu tun?
Der Justizminister sollte die neuen Regelungen so anwenden, daß unverhältnismäßige Eingriffe in die Grundrechte der Gefangenen vermieden werden.

4.4.3 Zentrale Register der Staatsanwaltschaften

Trotz der Einführung des Verfahrens MESTA bei allen fünf Staatsanwaltschaften des Landes sind noch einige Fragen zur Datensicherheit und des Datenschutzes offen. Erreicht werden konnte, daß die Daten in Schleswig-Holstein auf dem Übertragungsweg verschlüsselt werden.

Im 20. Tätigkeitsbericht (Tz. 4.4.1) hatten wir berichtet, daß das Verfahren MESTA bei der Staatsanwaltschaft Flensburg in den **Pilotbetrieb** gegangen war. Mittlerweile sind alle Staatsanwaltschaften des Landes mit entsprechenden Systemen ausgestattet. Zur Zeit gibt es allerdings noch eine Reihe technischer Probleme, so daß von einem Normalbetrieb noch nicht die Rede sein konnte. Aus diesem Grund sind noch einige datenschutzrechtlich relevante Fragen offen.

Insbesondere muß in den einzelnen Staatsanwaltschaften noch geklärt werden, wie die **Zugriffsrechte** der **einzelnen Mitarbeiter** auf die Daten konkret ausgestaltet werden. Sie müssen grundsätzlich streng auf die jeweiligen Zuständigkeiten beschränkt sein, ohne die Möglichkeit zu verbauen, kurzfristig auf Vertretungssituationen und auf die bei den Staatsanwaltschaften regelmäßig vorkommende Sitzungsvertretung zu reagieren.

Ein Erfolg unserer datenschutzrechtlichen Bemühungen zeichnet sich bereits ab: Die Notwendigkeit der **Datenverschlüsselung** auf dem Übertragungsweg haben inzwischen auch das Justizministerium und die Generalstaatsanwaltschaft erkannt,

allerdings noch nicht realisiert. Sie beabsichtigen, den Datenabgleich, der regelmäßig zwischen den verschiedenen Staatsanwaltschaften durchgeführt wird, nur in verschlüsselter Form über die Leitungen des Schleswig-Holstein-Netzes zu schicken.

Anfang 1999 ist das **„Zentrale Staatsanwaltschaftliche Verfahrensregister"** (ZStV) in Betrieb gegangen, über das wir im 18. Tätigkeitsbericht (Tz. 4.4.2) berichtet hatten. Damit soll es allen Staatsanwaltschaften im Bundesgebiet möglich sein, festzustellen, ob gegen bestimmte Beschuldigte bereits bei anderen Staatsanwaltschaften Verfahren eröffnet wurden. Das ZStV wird ebenso wie das Bundeszentralregister (BZR) von der Generalbundesanwaltschaft in Berlin geführt. Sämtliche Staatsanwaltschaften in Deutschland sind verpflichtet, die neu eröffneten Ermittlungsverfahren an das ZStV mitzuteilen. In MESTA steht bereits eine entsprechende Schnittstelle zur Verfügung. Allerdings sind andere Bundesländer mit der Ausgestaltung ihrer landeseigenen staatsanwaltschaftlichen Systeme noch nicht so weit, so daß das ZStV wohl erst in zwei Jahren vollständige Daten über sämtliche in der Bundesrepublik begonnenen Strafverfahren enthalten wird. Von datenschutzrechtlichem Interesse ist, daß die Speicherungsdauer im ZStV auf zwei Jahre nach rechtskräftiger Entscheidung im Strafverfahren beschränkt und somit kürzer als in MESTA ist (vgl. 20. TB, Tz. 4.4.1).

Was ist zu tun?
Beim Einsatz von MESTA im täglichen Betrieb und insbesondere bei der Vergabe der Zugriffsrechte müssen noch datenschutzrechtliche Vorgaben umgesetzt werden.

4.4.4 Fehler im Schuldnerverzeichnis

Es kann zu gravierenden wirtschaftlichen Folgen für Betroffene kommen, wenn Informationen aus dem Schuldnerverzeichnis nicht korrekt gehandhabt werden. Wie schwer es ist, eine fehlerhafte Eintragung im Schuldnerverzeichnis wieder „einzufangen", müssen dann die Betroffenen erfahren.

- **Löschung eines Haftbefehls im Schuldnerverzeichnis – bei der Bank nicht angekommen?**

Ein säumiger Schuldner war von seiner Bank zur Abgabe der **eidesstattlichen Versicherung** vor dem Amtsgericht aufgefordert worden. Kurz vor dem Termin einigten sich die Parteien jedoch über Rückzahlungsmodalitäten; ein entsprechendes Fax der Bank an das Amtsgericht gelangte offensichtlich nicht auf den Tisch des zuständigen Richters, so daß dieser wegen des Ausbleibens des Schuldners Haftbefehl erließ. Dieser wurde prompt in das Schuldnerverzeichnis eingetragen und per Abdruck an eine Reihe von Wirtschaftsauskunfteien übermittelt. Nach Zustellung des Haftbefehls veranlaßte der Schuldner sofort dessen Aufhebung und Löschung im Schuldnerverzeichnis. Dem wurde ebenso prompt entsprochen; Nachtragsmitteilungen gingen auch an die Empfänger der Abdrucke.

Zwischenzeitlich konnte der Petent als selbständiger Handelsvertreter eine neue Arbeit finden und seine finanzielle Situation bereinigen. Um für seine Tätigkeit einen **Überziehungskredit** zu vereinbaren, sprach er bei seiner neuen Bank vor. Diese lehnte jedoch nach Blick auf den Bildschirm des Computers mit den Worten ab: „Bringen Sie erst einmal die Sache mit dem Haftbefehl in Ordnung!" Auch nachdem der Betroffene die Zusammenhänge um den versehentlich entstandenen Haftbefehl erläutert hatte, blieb man dabei: „Da wird schon irgend etwas gewesen sein. In Deutschland wird man nicht so ohne weiteres verhaftet. Ihren Antrag auf einen Überziehungsrahmen lehnen wir ab!"

Warum die Information über den zwischenzeitlich gelöschten Haftbefehl noch bei dieser Bank – und möglicherweise anderen Stellen – vorhanden war, obwohl die Löschungsmitteilungen korrekt an die Abdruckempfänger versandt worden waren, war auch durch das Innenministerium im Rahmen der Aufsicht über den Privatbereich letztlich nicht mehr zu klären.

- **Per Mausklick ins Schuldnerverzeichnis**

Eine Petentin beabsichtigte im September 1998 für ihre neu gegründete Firma einen Pkw zu leasen. Ein entsprechender Vertrag kam jedoch nicht zustande, da ihr vom Autohaus vorgehalten wurde, bei der **SCHUFA** gespeichert zu sein. Sie fiel aus allen Wolken.

Was war geschehen? Gegen die Petentin wurde im März 1998 ein Zwangsvollstreckungsverfahren eingeleitet, das jedoch im April wieder eingestellt wurde. Im zuständigen Amtsgericht war sie im März ordnungsgemäß mit den Daten aus diesem Verfahren im **System MEGA** gespeichert worden. Dort wird ein automatisches Vollstreckungsregister geführt, das sich in zwei Unterregister unterteilt: eines für Verfahren, in denen eine eidesstattliche Versicherung abgegeben wird (M1), und eines für sonstige Vollstreckungssachen (M2). Um den Bearbeitern die Eingabe zu erleichtern, sieht MEGA **ein Verfahrensregister** mit sämtlichen Vollstreckungsverfahren vor. Dadurch können Grunddaten, die bereits einmal eingegeben wurden, für ein weiteres Verfahren automatisch übernommen werden.

Im April 1998 beabsichtigte eine Mitarbeiterin des Amtsgerichts, das Datum der Abgabe einer eidesstattlichen Versicherung in einen Datensatz zu einem **Namensvetter** der Petentin einzugeben. Aus Unachtsamkeit erzeugte sie jedoch anstatt dessen einen Schuldnerverzeichniseintrag zu der Petentin. Durch die in diesem Bereich **nicht ausgereifte Technik** im Verfahren MEGA wurde ihr die Falscheingabe wesentlich „erleichtert". Über den Namen als Suchmodus kam man nämlich in das oben erwähnte Verfahrensgesamtregister, in dem auch der Name der Petentin mit dem Aktenzeichen aus dem Zwangsvollstreckungsverfahren aufgeführt war. Versehentlich rutschte die Mitarbeiterin mit dem Cursor auf die Zeile mit dem Namen der Petentin und klickte ihn an. Auf der nächsten Maske erschienen die Personengrunddaten, die jedoch von der Mitarbeiterin des Amtsgerichts nicht mehr abgeglichen wurden. Sie klickte sofort zur nächsten Maske weiter, in der das Datum der Abgabe der eidesstattlichen Versicherung eingegeben wird. Diese Maske legt sich über die vorherige Maske, so daß die Grunddaten dann

nicht mehr sichtbar sind.

Aber ein Fehler kommt selten allein. Einige Tage nach dem Versand der Abdrucke aus dem Schuldnerverzeichnis rief eine Mitarbeiterin eines der Abnehmer an, weil sie sich über das untypische Aktenzeichen und das fehlende Geburtsdatum zu dem Eintrag der Petentin gewundert hatte. Die Mitarbeiterin bemerkte ihren Eingabefehler und wollte diesen umgehend beseitigen. Daher griff sie kurzerhand zum Telefonhörer und meldete die Löschung der Petentin aus dem Schuldnerverzeichnis an die Abnehmer der Abdrucke weiter. Dabei ließ sie die Vorschriften der **Schuldnerverzeichnisverordnung**, die eine schriftliche Löschungsmitteilung zwingend vorsieht, unberücksichtigt. Ein Abnehmer reagierte offensichtlich nicht auf die telefonische Löschung und wartete eine schriftliche Mitteilung ab, so daß die Petentin bis September 1998 weiterhin bei der SCHUFA gespeichert war.

Das für die Programmierung von MEGA zuständige Justizministerium hat diesen Vorfall bereits zum Anlaß genommen, das Verfahren nachzubessern. Künftig wird das M1-Register weiter unterteilt in eine Liste mit Schuldnern, die bereits eine eidesstattliche Versicherung abgegeben haben, und in eine Liste mit sonstigen Schuldnern. Ferner wird ausschließlich innerhalb des M1-Registers eine Übersichtsliste der Verfahren eingerichtet, so daß dort nur „Schuldnervorgänge" geführt werden. Des weiteren erscheint bei der Eingabe eines eidesstattlichen Versicherungsdatums eine zusätzliche **rot umrandete Maske** mit der Aufforderung, die Personendaten noch einmal zu kontrollieren, da die Eintragung zur Aufnahme in das Schuldnerverzeichnis führt. Damit sind Fehleintragungen wie im vorliegenden Fall künftig nicht mehr so leicht möglich. Menschliches Versagen kann natürlich niemals gänzlich ausgeschlossen werden.

Was ist zu tun?
Beim Umgang mit Daten aus dem Schuldnerverzeichnis ist größtmögliche Sorgfalt geboten. Durch zusätzlichen Anwenderkomfort dürfen nicht auf der anderen Seite datenschutzrechtliche Risiken entstehen.

4.5 Ausländerüberwachung – ein gesellschaftliches Pilotprojekt?

4.5.1 Überblick

Im unserem 17. Tätigkeitsbericht (Tz. 4.1.3) wurden datenschutzrechtliche Probleme in der Ausländer- und Asylverwaltung dargestellt. Schon damals war von der Asylcard oder von der zentralen Erfassung im Ausländerzentralregister zu berichten. Zum **Ausländerzentralregister** machte noch die alte Bundesregierung weitergehende Regelungsvorschläge: Statt die Nutzung dieses – aus verfassungsrechtlicher Sicht fragwürdigen – multifunktionalen Registers auf ausländerrechtliche Zwecke zu beschränken, war eine Ausweitung um eine sozialrechtliche Komponente geplant. Zudem sollte eine sogenannte **Warndatei** in Form einer reinen Verdachtsdatei eingerichtet werden, mit der Täuschungen bei der Visaerteilung und kriminelle Schleusertätigkeit verhindert werden sollten.

Eine Gesamtsicht der Erfassungsinstrumente in bezug auf Ausländerinnen und Ausländer ergibt, daß es sich hierbei um die **am intensivsten durchleuchtete Bevölkerungsgruppe** in Deutschland handelt. Es drängt sich immer wieder der Eindruck auf, als würden an dieser Gruppe neue Überwachungsinstrumente erprobt, die, wenn sie sich „bewährt" haben, auch gegenüber anderen Menschen eingesetzt werden.

4.5.2 Asylcard – zwischen Verwaltungseffizienz und Totalkontrolle

Nach jahrelangen Vorüberlegungen ist die Diskussion über die Einführung einer Asylcard in ein konkretes Stadium getreten. Die im Auftrag des Bundesministers des Innern erstellte Machbarkeitsstudie weist erhebliche Mängel auf.

Die vom Bundesministerium des Innern in Auftrag gegebene Machbarkeitsstudie zur Einführung einer **Asylcard** liegt nun vor. Zwar bemühen sich die Autoren dem Eindruck entgegenzutreten, mit der „Smart-Card" solle in erster Linie die Kontrolldichte bei Flüchtlingen erhöht werden. Zweck sei es vielmehr, die Aktualität und Richtigkeit der bestehenden Dateien sowie die Kommunikation zwischen den verschiedenen beteiligten Behörden zu verbessern. Tatsächlich würde aber mit dieser Chipkarte die Totalkontrolle der Flüchtlinge möglich. Die Asylcard soll nämlich nicht nur als Ausweis genutzt werden, sondern auch als Datenspeicher für die Kommunikation zwischen Ausländerbehörden, Sozialbehörden, Arbeits- und Meldeämtern, den Aufnahmeeinrichtungen und dem federführenden Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl). Jeder dieser Behörden soll auf der Karte eine sogenannte zweckgebundene Anwendung reserviert werden, auf die auch andere Behörden zugreifen könnten, wenn der Betroffene seine Karte vorlegt. Für die eindeutige Identifizierung ist die elektronische Speicherung eines **Fingerabdrucks** vorgesehen. Um sich auszuweisen, sollen die Flüchtlinge die Karte ins Lesegerät stecken und zugleich einen bestimmten Finger auf ein Lesegerät legen, das diesen mit den auf der Karte gespeicherten Fingerlinien (Minuzien) vergleicht.

Die Studie setzt sich nur sehr unzureichend mit den Rahmenbedingungen und Konsequenzen des Karteneinsatzes auseinander.

- Eine **Vielzahl von Gesetzen**, vom Asyl- über das Melde- bis zum Sozialrecht, müßten geändert werden.
- Die Frage nach der **Erforderlichkeit** der vorgesehenen Datenabrufe von der Karte wird ungenügend beantwortet; Datenzugriffe sollen erlaubt werden, die zur Aufgabenerfüllung gar nicht nötig sind.
- Die **Polizei** soll praktisch auf sämtliche Kartendaten zugreifen können.
- **Unzureichend** sind auch die in der Studie vorgesehenen technischen und organisatorischen **Vorkehrungen** zur Verhinderung unzulässiger Zugriffe, zur Information der Betroffenen und zur Absicherung sogenannter Hintergrundsysteme.

- Besonders gravierend erscheint uns die Anwendung „**Aufenthaltssteuerung**".

Es waren keine Vorkehrungen vorgesehen, um ein in Holland bereits praktiziertes Verfahren auszuschließen, bei dem die Flüchtlinge durch strenge Meldepflichten an sogenannte Meldesäulen einer fast **totalen Aufenthaltskontrolle** in der Art eines „Gefängnisses ohne Mauern" unterworfen werden. Es ist nicht auszuschließen, daß die Auftraggeber der Studie ähnliches im Sinn führen.

Wir haben deshalb dem Innenminister dringend von der Verwirklichung der Asylcardpläne abgeraten. Relativ unproblematisch wäre dagegen die Einführung eines fälschungssicheren, opto-elektronisch lesbaren, **einfachen Flüchtlingsausweises** ähnlich dem deutschen Personalausweis. Mit einem solchen, erheblich billigeren Mittel wären die größten Probleme der Identitätssicherung und der Verhinderung paralleler Verfahren lösbar. Die Entscheidung hierüber steht noch aus.

Was ist zu tun?
Die Pläne einer multifunktionalen Asylcard sollten zugunsten eines fälschungssicheren Flüchtlingsausweises fallengelassen werden.

4.5.3 EURODAC

Die Verantwortlichkeiten für die geplante europaweite Fingerabdruckdatei für ausländische Flüchtlinge EURODAC sind noch völlig unklar. Das gilt auch für die Datenschutzkontrolle.

Unter dem Kürzel „EURODAC" planen die Innenministerien der EU eine gemeinsame Fingerabdruckdatei einzurichten, um ausländische Flüchtlinge eindeutig zu identifizieren und um zu verhindern, daß unter einem anderen Namen in einem anderen EU-Mitgliedstaat ein zweiter Asylantrag gestellt wird. Mit dem EURODAC-Abkommen soll das Dubliner Übereinkommen umgesetzt werden, wonach innerhalb der EU für einen Asylantrag nur ein Staat zuständig sein soll. Statt wie bei anderen europäischen Dateien, z. B. dem Schengener Informationssystem oder bei Europol, eine eigene Verantwortlichkeit der europäischen Ebene zu begründen, soll bei EURODAC **Datenverarbeitung im Auftrag** der Mitgliedstaaten erfolgen. Dies wäre dann logisch, wenn die Mitgliedstaaten auch die ausschließliche Bestimmungsbefugnis über die gespeicherten Daten hätten. Dies ist aber nicht geplant. Vielmehr sollen automatisierte Abrufe möglich sein, ohne daß der dateneingebende Staat hierauf Einfluß nehmen könnte. Abfrage und Eingabe sollen automatisiert möglich sein, ohne daß die bei entsprechenden deutschen automatisierten Verfahren üblichen Sicherheitsstandards im Entwurf vorgesehen sind. Zudem sollen von mehr Personen als bisher in Deutschland Fingerabdrücke erfaßt werden, z. B. von Personen mit Aufenthaltsgenehmigung, bei denen regelmäßig keine Zweifel an der Identität bestehen. Die von deutscher Seite zusätzlich erhobene Forderung, auch andere als asylsuchende Ausländer zu erfassen, würde den Anwendungsbereich über das Dubliner Übereinkommen hinaus noch weiter aufblähen.

Besonders problematisch ist, daß **keine Kontrolle der Datennutzung** sichergestellt ist, wenn die Daten erst einmal abgefragt werden. So würde es leicht möglich, die Fingerabdrücke aus anderen EU-Staaten ohne weitere Voraussetzungen für die Strafverfolgung nutzbar zu machen. Dies böte sich geradezu an, da – obwohl für den eigentlichen Speicherzweck nicht erforderlich – sämtliche zehn Finger daktyloskopisch erfaßt werden. Damit verbunden wäre eine europaweite Stigmatisierung von Asylsuchenden als potentielle Straftäter. Wir haben vorgeschlagen, ein in der Kriminaltechnik nicht eingesetztes biometrisches Verfahren zur eindeutigen Identifizierung, z. B. über eine Erkennung der Iris oder der Augennetzhaut, zu verwenden. Das Risikopotential der EURODAC-Datei erhöht sich dadurch, daß selbst nach erfolgter Asylanerkennung keine Löschung geplant ist.

Zu kritisieren war schließlich die geplante Datenschutzaufsicht durch eine „**Gemeinsame Kontrollinstanz**". Hierdurch würde der Kompetenzwirrwarr bei der Datenschutzkontrolle auf europäischer Ebene weiter gefördert; außerdem entstünde die Gefahr von Kontrollücken mangels ausreichender Kompetenzen dieser Kontrollinstanz.

Was ist zu tun?
Der Entwurf des EURODAC-Abkommens muß vor Einleitung des Ratifikationsverfahrens umfassend überarbeitet werden.

4.5.4 Datenabgleich im Asylbewerberleistungsgesetz

Kurz vor der Bundestagswahl beseitigte der Bundesgesetzgeber im Schnelldurchgang noch einige „Datenschutzhindernisse" für die Verwaltung. Betroffen war davon vor allem das Asylbewerberleistungsgesetz.

Die Behörden, die Asylbewerbern Leistungen gewähren, seien, so die Argumentation des Bundesrates im Gesetzgebungsverfahren, oft nur schwer in der Lage, die Identität der Leistungsempfänger festzustellen. Konkrete Zahlen oder Belege hierfür wurden nicht vorgelegt. Von uns vorgeschlagene datenschutzfreundliche Lösungen, z. B. die Ausgabe fälschungssicherer Ausweispapiere, wurden im Gesetzgebungsverfahren erst gar nicht erörtert. Vielmehr nahm man die Problemlösung an den Betroffenen vor: durch einen **Datenabgleich** mit der Ausländerbehörde. Das Problem ist, daß dabei die Leistungsträger nicht nur über das erforderliche Maß hinaus Daten der Ausländerbehörden erhalten, sondern umgekehrt zugleich Informationen über den Leistungsbezug liefern, die die Ausländerbehörden nicht benötigen.

Nicht gelöst wurde das datenschutzrechtliche Hauptproblem des Asylbewerberleistungsgesetzes. Durch dessen **Herauslösung aus dem Sozialleistungsrecht** sind weder das Sozialgeheimnis noch die sozialrechtlichen Übermittlungsregelungen anwendbar. Es muß daher auf das allgemeine Datenschutzrecht zurückgegriffen werden, das auf die Sensibilität von Informationen über soziale Hilfen nicht zugeschnitten ist.

4.5.5 Verwaltungsvorschriften zum Ausländergesetz

Bund und Länder haben es in acht Jahren nicht geschafft, sich auf einheitliche Verwaltungsvorschriften zum Ausländergesetz zu verständigen. Noch sind 200 Positionen offen.

Als 1990 das derzeit gültige Ausländerrecht in Kraft trat, war von Anfang an klar, daß dessen teilweise äußerst unbestimmte Regelungen einer **Konkretisierung in Verwaltungsvorschriften** bedürfen. Diese liegen bis heute nicht vor. Bundesregierung und Bundesrat waren im Verlaufe von acht Jahren nicht dazu in der Lage, gemeinsam die notwendigen Verwaltungsvorschriften zum Ausländergesetz zu erlassen. Ein Unterausschuß des Bundesrates behandelte zuletzt knapp zweihundert Änderungsvorschläge zum Entwurf des Bundesinnenministeriums. Ob die neue Bundesregierung den Entwurf weiterverfolgt, ist noch nicht klar.

Aus Datenschutzsicht ist von zentraler Bedeutung, daß die wegen ihrer Unbestimmtheit und Weite verfassungsrechtlich problematischen **Regelungen** zur Datenverarbeitung **vernünftig eingegrenzt** werden. Wir haben deshalb noch einmal unsere Vorstellungen gegenüber dem Innenministerium vorgetragen:

- Unterrichtung der Betroffenen bei der Datenerhebung bei Dritten zur Verbesserung der Transparenz,
- Vermeidung von Interessenkonflikten bei der Umsetzung der Übermittlungspflicht von im Bildungs-, Gesundheits- und Sozialbereich tätigen öffentlich Bediensteten,
- Klärung der Verantwortlichkeit bei Datenübermittlungen auf Ersuchen,
- Annahme der Übermittlungspflicht nur bei der sachnächsten Stelle,
- Beschränkung dieser Pflicht auf konkrete Ausweisungsfälle,
- Berücksichtigung des Verhältnismäßigkeitsgrundsatzes bei Datenübermittlungen z. B. aus dem Sozialbereich,
- Vermeidung der Offenbarung personenbezogener Daten von einladenden Personen.

Was ist zu tun?
Die Verwaltungsvorschriften sind nun endlich in einer den verfassungsrechtlichen Anforderungen genügenden Fassung in Kraft zu setzen.

4.6 Wirtschaft, Technik, Verkehr

4.6.1 Ausführungsgesetz zur Insolvenzordnung

Seit Anfang 1999 gilt ein völlig neues Verfahren bei Insolvenzen von Privatpersonen. Durch das schleswig-holsteinische Ausführungsgesetz werden die sensiblen Schuldnerdaten besonders geschützt.

Durch das neue Verfahren zur Verbraucherinsolvenz erhalten „geeignete Stellen" die Aufgabe der Durchführung der **außergerichtlichen Schuldenregulierung** für Verbraucher. Hierbei soll ein Interessenausgleich zwischen Schuldnern und Gläubigern mit dem Ziel der vollständigen Schuldenfreiheit nach Ablauf von sieben Jahren erreicht werden. So sehr diese Neuregelung im Interesse der Verbraucher zu begrüßen ist, so ist doch zu bedenken, daß bei diesem Verfahren hochsensible Daten anfallen: Angaben zu den finanziellen Verhältnissen, Hintergründe der Verschuldung, familiäre und persönliche Konflikte, Alkohol- oder sonstiger Drogenkonsum, Probleme am Arbeitsplatz, Kriminalität usw.

Natürlich muß hier „Datenschutz" besonders groß geschrieben werden. Weil privatrechtlich organisierte **Schuldnerberatungsstellen** nach dem Bundesdatenschutzgesetz überhaupt keinem Datenschutzrecht unterliegen würden, wenn sie die Daten nur in Akten verarbeiten, haben wir dem Landtag vorgeschlagen, sie generell dem **Landesdatenschutzgesetz** zu unterwerfen. Der Landtag ist diesem Vorschlag gefolgt, so daß auch private Schuldnerberatungsstellen wie öffentliche Stellen behandelt werden. Dies hat für die Betroffenen eine Vielzahl von Vorteilen: Die Daten unterliegen einer strengen Zweckbindung; die Datenschutzkontrolle wird von uns wahrgenommen, ohne daß es einer konkreten Beschwerde bedarf; auch sensible Daten in Akten werden geschützt. Zudem wird dadurch sichergestellt, daß bei privaten und öffentlichen Schuldnerberatungsstellen kein unterschiedliches Datenschutzrecht gilt.

Was ist zu tun?
Die „Schuldnerberatungsstellen" haben ihre Mitarbeiterinnen und Mitarbeiter über die Anforderungen des Landesdatenschutzgesetzes zu unterrichten und die notwendigen technischen und organisatorischen Sicherheitsvorkehrungen zu treffen.

4.6.2 Notwendige Kammermitteilung oder öffentlicher Pranger?

Bundesweit war es bei den Steuerberaterkammern Praxis, wettbewerbsrechtliche Gerichtsurteile gegen einzelne Personen zu veröffentlichen. In Schleswig-Holstein wird dies künftig unterbleiben.

Den Steuerberatern sollte durch die Veröffentlichung von Gerichtsurteilen über die Untersagung von Steuerberatungstätigkeiten die Möglichkeit gegeben werden, die Einhaltung der Unterlassungserklärungen zu kontrollieren und Verstöße hier-

gegen der Kammer anzuzeigen. Diese Praxis stieß natürlich auf wenig Gegenliebe bei den Betroffenen, die sich **öffentlich bloßgestellt** fühlten. Sie baten uns um Klärung der Frage, ob die Veröffentlichung ihrer Namen zulässig war. Sie berichteten, daß die Mitteilungen von Steuerberatern in einzelnen Fällen auch dazu genutzt wurden, den nicht zugelassenen Buchprüfern anzubieten, der abgemahnten Tätigkeit unter ihrem Firmenmantel nachzugehen.

Bei der Veröffentlichung der Daten in einer Zeitschrift handelt es sich um eine **Übermittlung** an nichtöffentliche Stellen. Auch wenn es zu den Aufgaben der Kammer gehört, die Interessen ihrer Mitglieder zu vertreten, so ist hieraus nicht die Befugnis abzuleiten, derartige Veröffentlichungen vorzunehmen. Von den in Schleswig-Holstein durch die Steuerberaterkammer erstrittenen Unterlassungserklärungen waren ca. 10 % „Wiederholungsfälle". Selbst in diesen Fällen führten nicht die Veröffentlichungen in den Kammermitteilungen zur Anzeige. Die Kammer **verzichtet** nach unserer Intervention in Zukunft auf die personenbezogene Veröffentlichung erwirkter Unterlassungserklärungen. Die Sachverhalte sollen in einer Form dargestellt werden, die eine Zuordnung zu konkreten Personen nicht mehr ermöglicht. Auch in anderen Ländern konnten die Datenschutzbeauftragten die Steuerberaterkammern zu einer Änderung ihrer Praxis bewegen.

Was ist zu tun?
Die Veröffentlichung wettbewerbsrechtlicher Unterlassungserklärungen muß künftig in einer Form erfolgen, bei der keine Rückschlüsse auf konkrete Personen möglich ist.

4.6.3 Alle Autobahngegner auf einen Blick

Der Neubau der Autobahn von Lübeck nach Rostock wirft nicht nur ökologische und politische Probleme auf. Im Planfeststellungsverfahren wurden auch datenschutzrechtliche Standards nicht beachtet.

Der über 300 Seiten dicke **Planfeststellungsbeschluß** für den ersten Streckenabschnitt der A 20 hatte datenschutzrechtliche Haken. Auf 14 eng bedruckten Seiten wurden die Namen **aller Einwenderinnen und Einwender** aufgelistet. Mitgeliefert wurden teilweise auch Adresse, Flurstücknummer sowie genaue Angaben zu den örtlichen und persönlichen Gegebenheiten. Erkennbar war auch, ob sich ganze Familien dem Straßenprojekt widersetzen. Zwar wurden einzelne Einwendungen im Interesse des Persönlichkeitsschutzes gesondert beschieden. Im zentralen Beschlußtext unterblieb aber jede Form der **Anonymisierung bzw. Pseudonymisierung**. Kein Wunder, daß dies einigen Betroffenen nicht gefiel.

Im Jahr 1990 hat das Bundesverfassungsgericht entschieden, daß es für eine ordnungsgemäße Begründung von Planfeststellungsbeschlüssen nicht erforderlich ist, daß die geltend gemachten Einwendungen personenbezogen veröffentlicht werden. Unter dem Gesichtspunkt des Rechtsschutzes der Betroffenen genüge es, daß den Betroffenen eine **Nummer** bekannt gegeben werde, unter der ihre Daten in den Planfeststellungsbeschluß aufgenommen worden sind. Auf diese Weise

können individuelle Einwendungen der jeweiligen Person richtig zugeordnet werden.

Diese Rechtsprechung wurde vom Landesamt für Straßenbau ignoriert. Auf unsere Beanstandung hin sagte es jetzt zu, in Zukunft Planfeststellungsbeschlüsse hinreichend zu anonymisieren. Die Einwender werden bei der Zustellung des Beschlußtextes über ihre jeweilige Kennziffer individuell informiert.

Was ist zu tun?
Bei der Veröffentlichung von Planfeststellungsbeschlüssen ist darauf zu achten, daß die personenbezogenen Angaben über Einwender verschlüsselt dargestellt werden.

4.6.4 „Videokameras" an Autobahnbrücken?

An vielen Autobahnbrücken sind in den letzten Monaten technische Systeme, die Videokameras ähneln, installiert worden. Bürger wandten sich mit der Frage an uns, ob dies der Auftakt zur totalen Überwachung sei.

An vielen Autobahnbrücken wurden im vergangenen Jahr solarbetriebene Geräte für ein **Verkehrsinformations- und Leitsystem** installiert. Diese Geräte sehen aus wie Videokameras und veranlaßten Bürger zu der Annahme, daß es sich hierbei um neue Überwachungsgeräte handelt, mit denen womöglich Bewegungsprofile erstellt werden können. Unsere Anfrage beim Verkehrsministerium ergab, daß das von einer Privatfirma betriebene System lediglich die Anzahl der die Meßgeräte passierenden Fahrzeuge und deren Geschwindigkeit erfaßt. Diese Informationen werden z. B. als Grundlage für Staumeldungen im Rundfunk benutzt.

Darüber hinaus werden diese Daten der Straßenbauverwaltung für statistische und planerische Zwecke überlassen. Auch die Straßenverkehrsbehörden, die Polizei und die Katastrophenschutzbehörden können diese Informationen nutzen. Ein **Personenbezug** kann mit ihnen jedoch **nicht hergestellt** werden. Aus den uns vorliegenden Verträgen zwischen den beteiligten Stellen ist auch nicht die Absicht erkennbar, künftig das individuelle Fahrverhalten zu überwachen. Das Verfahren ist also derzeit datenschutzrechtlich unbedenklich.

4.6.5 Zulassungsstellen sind keine Dienstleister für Versicherungen

Es gehört nicht zu den Aufgaben von Zulassungsbehörden, Kfz-Versicherungen von sich aus anläßlich der Vorlage von Versicherungsdoppelkarten vor möglichen Betrügern zu warnen.

Eine Kraftfahrzeugzulassungsbehörde erhielt von der Polizei den Hinweis, daß eine bestimmte Person womöglich unter Vorlage einer erschlichenden Versicherungsbescheinigung (sogenannte **Versicherungsdoppelkarte**) ein Fahrzeug anmelden wolle. Dieser Hinweis wurde gespeichert. Als der Betroffene tatsächlich

in der Zulassungsstelle erschien, um ein Fahrzeug anzumelden, setzte sich der Sachbearbeiter mit der Versicherung in Verbindung. Diese teilte mit, sie sei nicht bereit, das Fahrzeug zu versichern. Er versuchte es daraufhin erneut unter Vorlage der Versicherungsdoppelkarte einer anderen Versicherung. Der Vorgang wiederholte sich: Auch diese Versicherung verweigerte auf Nachfrage durch die Zulassungsbehörde den Versicherungsschutz. Der Betroffene vertrat die Ansicht, die Zulassungsbehörde müsse ein Fahrzeug zulassen, wenn eine Versicherungsdoppelkarte vorgelegt werde. **Rückfragen** bei der Versicherung seien **unzulässig**.

Tatsächlich ist die Zulassungsbehörde nach den Vorschriften der Straßenverkehrszulassungsordnung nicht berechtigt, die Gültigkeit einer korrekt ausgefüllten Versicherungsdoppelkarte einer Versicherung anzuzweifeln und bei der Versicherung nachzufragen. Dies gilt selbst dann, wenn der Zulassungsbehörde Hinweise vorliegen, daß der Betreffende tatsächlich verdächtig ist, Betrugsdelikte im Zusammenhang mit Kfz-Versicherungen begangen zu haben. Das Verkehrsministerium teilt unsere Rechtsauffassung. Der Gesetzgeber geht nämlich davon aus, daß die **Kfz-Versicherungen** bei der Ausgabe der Versicherungsdoppelkarten im eigenen Interesse ausreichende Sorgfalt walten lassen müssen und nur denjenigen Personen einen Versicherungsnachweis für die Zulassungsstellen aushändigen, mit denen sie auch tatsächlich einen Versicherungsvertrag abschließen wollen. Wir haben deshalb die Verfahrensweise der Zulassungsbehörde beanstandet. Diese teilte uns daraufhin mit, sie werde zukünftig entsprechende Rückfragen bei den Versicherungen unterlassen.

4.7 Sozialbereich

4.7.1 Überblick

Als das Bundesverfassungsgericht 1983 im Volkszählungsurteil bereichsspezifische Datenschutzregelungen forderte, bezeichnete es den **Sozialdatenschutz** als beispielhaft und richtungsweisend. Diese Einschätzung würden sich die höchsten deutschen Richter wohl verkneifen. Zu viele Gesetzgebungs- und tatsächliche Veränderungen sind über diesen Bereich hinweggegangen, als daß man das Sozialgeheimnis noch als das erkennen könnte, was es einmal war. Immer wieder wurden **neue** gesetzliche **Durchbrechungen zugelassen**. So wurde z. B. mit dem Asylbewerberleistungsgesetz die Gruppe der Flüchtlinge komplett aus dem Geltungsbereich des Sozialgeheimnisses herausgenommen. Zuletzt erhielt die Polizei den Zugriff auf die Aufenthaltsdaten bei allen Sozialleistungsträgern (dazu Tz. 4.7.3). Grundidee des Sozialgeheimnisses ist es, Hilfsbedürftigen existenzsichernde Leistungen zukommen zu lassen, ohne daß sie deshalb Diskriminierungen oder sonstige schwerwiegende Nachteile befürchten müßten.

Angesichts knapper Kassen ist es ein legitimes Bedürfnis, ungerechtfertigte Sozialleistungen zu vermeiden. Dies führt zwangsläufig dazu, daß die Voraussetzungen für Hilfen penibel geprüft werden. Dies darf aber nicht so weit gehen, daß die Betroffenen einer Totalkontrolle unterworfen werden. Die neuerdings zulässigen Sozialhilfedatenabgleiche lassen nach ersten Ergebnissen darauf schließen,

daß es um die **Ehrlichkeit der Hilfeempfänger** besser bestellt ist als etwa mit der Steuerehrlichkeit. Übermäßige Kontrollen säen nicht nur Mißtrauen und sozialen Neid, sondern sie stellen einen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar, da Hilfsbedürftigkeit zumeist einen sehr persönlichen Hintergrund hat, der offengelegt wird. Hier ist Augenmaß angesagt. Das gleiche gilt für die einzelfallbezogene Prüfung der Anspruchsvoraussetzungen.



Im Bereich der Krankenversicherung sind die **Abrechnungs- und Kontrollverfahren** derart **kompliziert** geworden, daß sie von kaum jemandem mehr durchschaut werden können. Neben ausufernden Regelungen des fünften Sozialgesetzbuches (SGB) und der allgemeinen Vorschriften des zehnten Buches finden ergänzend noch eine Vielzahl von Vereinbarungen und Regularien der Spitzenverbände, der beteiligten Ministerien und der kassenärztlichen Vereinigungen Anwendung. Diese Regeln sind derart unübersichtlich, daß statt ihrer oft der „gesunde Menschenverstand" zur Anwendung kommt. Da es hier nicht „nur" um Daten, sondern vor allem auch um Geld geht, ist der Streit vorprogrammiert. Bei diesem Streit bleibt dann oft nicht nur das Sozialgeheimnis auf der Strecke, sondern auch die ärztliche Schweigepflicht.

4.7.2 Zum Stellenwert des Sozialgeheimnisses in der AOK Schleswig-Holstein

Von einer gesetzlichen Krankenversicherung muß erwartet werden, daß sie die Regelungen über den Sozialdatenschutz, die vor mehr als 20 Jahren im Sozialgesetzbuch verankert worden sind, strikt beachtet. Bei der AOK Schleswig-Holstein wurden jedoch gravierende Mängel festgestellt und beanstandet.

Einige Prüfungsmaßnahmen entwickeln sich ganz anders, als sie zunächst von uns geplant sind. Ein typisches Beispiel hierfür ist eine im März 1998 gestartete „Nachschau" bei der AOK Schleswig-Holstein. Da es sich bei dieser gesetzlichen Krankenversicherung um eine **Körperschaft öffentlichen Rechts** mit circa 80 „Lokationen" (Zentraldirektion, Bezirksdirektionen, Geschäftsstellen, Filialen, Außenstellen usw.) und mit insgesamt mehr als 2 500 Mitarbeitern handelt, erhielten die Prüfer den Auftrag, die sozialdatenschutzrechtlichen und die sicherheitstechnischen Gegebenheiten dieses Großunternehmens in einem Arbeitsgang zu durchleuchten.

Um das Ergebnis vorweg zu nehmen: Bis in die tieferen Schichten der Umsetzung des komplizierten Krankenversicherungsrechts nach dem Sozialgesetzbuch V und eines landesweiten Informations- und Kommunikationssystems für 2 500 vernetzte PC und ein Großrechenzentrum in Mecklenburg-Vorpommern sind wir im Verlaufe von fünf Monaten nicht vorgedrungen. Zu groß waren die vorrangig zu behebenden organisatorischen **Schwachstellen** bei der Gewährleistung des Sozialgeheimnisses und die **Sicherheitslücken** bei der automatisierten Verarbeitung personenbezogener Daten auf der Arbeitsplatzebene (zum letzteren vgl. Tz. 6.8.1).

Dabei ließ die vom **Vorstand** erlassene **Datenschutz-Dienstanweisung Vorbildliches** erwarten. In ihr wird nämlich in einer Art Präambel festgestellt, daß die gewissenhafte Beachtung von Datenschutz und Datensicherheit für die AOK ein sehr wichtiges Instrument sei, um das Vertrauen der Öffentlichkeit, insbesondere der Versicherten, Arbeitgeber und Vertragspartner dauerhaft zu sichern. Sie betrachte die Einhaltung dieser Verpflichtung, auch im Rahmen des Wettbewerbs um die Versicherten bei der Wahl ihrer Krankenkasse, als ein nicht unerhebliches Entscheidungskriterium. Der **Datenschutz** habe demzufolge einen sehr **hohen Stellenwert**. Von den Mitarbeiterinnen und Mitarbeitern wird deshalb gefordert: „Betrachten Sie den Datenschutz nicht länger als lästiges Hemmnis bei den zu verrichtenden Arbeiten, sondern als wesentliches **Element des Dienstleistungsauftrages der AOK** am Kunden. Der Datenschutz und die Wahrung des Sozialgeheimnisses sind für unsere AOK genauso wichtig wie beispielsweise ein richtiger und zeitnaher Leistungsservice." Die Dienstanweisung enthält circa zwei Dutzend Regelungen, die bezüglich ihrer Zielrichtung und Präzision einem Lehrbuch über Datensicherheit zur Ehre reichen würden.

Welch ein Unterschied aber zu den tatsächlichen Verfahrensweisen! Die **Prüfung** deckte zum Beispiel die folgenden **Mängel** auf:

- In keiner der kontrollierten Geschäftsstellen waren die **Diskretionszonen/Wartezonen** so ausgelegt, daß es nicht möglich war, Gespräche an den Beraterarbeitsplätzen mitzuhören.
- Die **Akustik** in einer neu und mit erheblichem finanziellen Aufwand eingerichteten Geschäftsstelle war so „gut", daß noch aus mehr als 10 Metern Entfernung ein Gespräch zwischen einer normal sprechenden Mitarbeiterin und einer älteren Dame von jedermann mitgehört werden konnte.
- In vielen Geschäftsstellen wurden die Mitarbeiter in die Situation gebracht, faktisch das Sozialgeheimnis zu verletzen, weil **Telefongespräche** aufgrund der räumlichen und akustischen Gegebenheiten von anderen Mitarbeitern, wartenden Kunden usw. mitgehört werden konnten. In einer Geschäftsstelle waren derartige Gespräche sogar gleichzeitig in den diagonal gegenüberliegenden Ecken des Raumes wahrnehmbar.
- Der **Abstand der Beratungsplätze** zueinander war in fast allen aufgesuchten Geschäftsstellen zu gering. In dieser Beziehung haben in der AOK offenbar keine geeigneten Überlegungen zum Sozialdatenschutz stattgefunden. Anders ist es nicht zu erklären, daß gerade in zwei neu konzipierten Geschäftsstellen die gravierendsten Probleme bestanden. Bezeichnend ist, daß Beraterarbeitsplätze nur noch mit einem Besucherstuhl ausgerüstet wurden. Würden, wie sonst üblich, zwei Besucherstühle vorgehalten, säßen von verschiedenen Sachbearbeitern betreute Versicherte weniger als einen Meter voneinander entfernt.
- Die von den Leitern der betreffenden Geschäftsstellen genannten Gründe für die von ihnen nicht bestrittenen **Defizite** bezogen sich in der Regel auf **Geld- und Raummangel**. Sie waren meistens nicht stichhaltig. Die Großraumbüros waren durchweg so dimensioniert, daß bei einer optimierten Platzausnutzung im nicht vom Publikum genutzten „hinteren Bereich" ausreichend große

Wartezonen eingerichtet werden konnten.

- Die **Bildschirme** der meisten Arbeitsplatzrechner waren so positioniert, daß sie von den benachbarten Bearbeitungsplätzen, teilweise sogar von den Wartezonen bzw. von außerhalb der Gebäude aus, **eingesehen** werden konnten. Dies war stets der Fall, wenn Kunden in den hinteren Bereich der Kundenberatungsräume gebeten wurden. Teilweise hatte man von einem Beratungsplatz aus gleich mehrere Bildschirme im Sichtfeld.

- Die **papierenen Unterlagen** mit personenbezogenen Daten lagerten in **offenen Regalen**, in nicht verschließbaren oder in nach Dienstschluß nicht verschlossenen Behältnissen. In einem Fall wurde das Fehlen verschließbarer Behältnisse mit Geldmangel begründet; in der gleichen Geschäftsstelle war jedoch – wozu auch immer – selbst der Arbeitsplatz des Hausmeisters mit einem vernetzten PC ausgerüstet. Das abendliche Abschließen der Schränke scheiterte in einer Geschäftsstelle daran, daß alle Schränke unterschiedliche Schlösser hatten. Der dadurch bedingte Zeitaufwand für das Auf- und wieder Abschließen wurde als unzumutbar angesehen. In einer anderen Geschäftsstelle lagerten ausgerechnet die besonders sensiblen Akten der **Pflegekasse**, die durchweg **ärztliche Gutachten** enthalten, in **offenen Regalen**. Dies war für jeden Besucher erkennbar, da sich oberhalb der Behältnisse das Schild „Pflegeversicherung" befand.

- Die Gebäude der Geschäftsstellen stellen sich als „offene Häuser" dar. **Besucher** können sich in ihnen **unbegleitet** bewegen. Dies wäre nur dann unbedenklich, wenn ausreichende Maßnahmen gegen die unbefugte Kenntnisnahme von Daten durch Dritte getroffen worden wären. Statt dessen waren **unverschlossene Türen** und Schränke, herumliegende Akten, aktive Bildschirme und übervolle Aktenböcke und Papierkörbe an der Tagesordnung.

- Bei einer bewußt einige Tage vorher **angekündigten Kontrolle** in einer Geschäftsstelle **nach Feierabend** wurde folgende Situation vorgefunden: Schränke waren **unverschlossen**, so daß auf Mitgliedschaftserklärungen von Versicherten einschließlich der Gesprächsvermerke der Mitarbeiter zugegriffen werden konnte. Die Körbe für den Postein- und -ausgang waren gefüllt und **offen zugänglich**. In unverschlossenen Karteischränken lagerten Unterlagen über kieferorthopädische Behandlungen einschließlich der entsprechenden ärztlichen Gutachten. Dies war vor dem Hintergrund zu beurteilen, daß die Geschäftsstelle gelegentlich als **Wahllokal** und einmal wöchentlich der Landesversicherungsanstalt als Beratungsstelle diente. Es wäre überraschend, wenn die Unterlagen zu diesen Zeiten besser gesichert würden als bei einer angekündigten Kontrolle durch den Landesbeauftragten für den Datenschutz.

- Es konnten keine Unterlagen vorgelegt werden, aus denen ein Konzept für die Vergabe von **Zugriffsberechtigungen** auf die zentrale Versichertendatenbank abgeleitet werden konnte. Es wurde lediglich erklärt, daß es Zugriffsbegrenzungen gäbe; man sei aber selbst mit dem Ergebnis nicht zufrieden. Dies liege auch an den **beschränkten Differenzierungsmöglichkeiten** der mehrere Jahre alten Software. Alle Stichproben zeigten, daß stets ein „größtmögliches" Datenprofil bereitgestellt wurde. Maßstab war der „denkbare Sonderfall" und nicht die „zwingende Notwendigkeit" des Alltags. Dies zeigte sich an einem Beispiel aus dem Bereich der Arbeitgeberbetreuung: Damit die **Außendienst-**

mitarbeiter in der Lage waren, komplexe Fragen nach der Dauer der Lohnfortzahlung bzw. der Krankengeldzahlung einzelfallbezogen zu beantworten, verfügten alle über den Zugriff auf die Diagnosedaten aller Versicherten im Lande. Sie besprachen also Probleme der Abführung von Sozialversicherungsbeiträgen mit Arbeitgebern und verfügten gleichzeitig über ein umfangreiches Wissen über den Gesundheitsstatus der Belegschaft des betreffenden und aller anderen Unternehmen.

- Wegen der Entscheidungsfreiheit der Mitglieder bei der Wahl der zu Beratungszwecken aufgesuchten Geschäftsstelle haben grundsätzlich alle Mitarbeiter der AOK einen **landesweiten Zugriff** auf alle Mitgliederdatensätze. Eine zielgerichtete **Protokollierung** und eine regelmäßige Auswertung von **Protokollierungen** erfolgte jedoch nicht. Im Ergebnis wußte niemand, welcher Mitarbeiter wann aus welchen Gründen auf welche Datensätze zugegriffen hatte.

Bei einer derartigen Diskrepanz zwischen Anweisungen und tatsächlichem Verhalten liegt der Schluß nahe, es handele sich um „menschliches Versagen" auf der ausführenden Ebene. In diesem Fall war das **Management** aber seit zwei Jahren über die Mängel **informiert**. Die aufgrund der Regelungen des Sozialgesetzbuches X bestellte interne **Datenschutzbeauftragte** hatte nämlich den **Vorstand** in ihren jährlichen Berichten im Detail bereits vor unserer Prüfung über viele Unzulänglichkeiten **unterrichtet**. Abhilfe wurde nicht geschaffen. Wir haben das als einen „erheblichen Mangel" angesehen und gemäß den Bestimmungen des Landesdatenschutzgesetzes hierüber das Ministerium für Arbeit, Gesundheit und Soziales unterrichtet.

Die AOK akzeptierte die ihr gegenüber ausgesprochenen Beanstandungen weitestgehend als berechtigt. Bereits während der Prüfung hat man damit begonnen, die Mängel abzustellen. In einer schriftlichen Stellungnahme ist zugesagt worden, bis Ende September 1999 alle diesbezüglichen Arbeiten zu einem Abschluß gebracht zu haben. In Anbetracht der Bedeutung der aufgezeigten Probleme bat uns die AOK, sie bei der Umsetzung der Vorhaben zu beraten, damit die gesetzlichen Anforderungen sachgerecht und praktikabel erfüllt werden.

Das Sozialministerium als Fachaufsichtsbehörde teilt unsere Bewertungen und hat angekündigt, die Behebung der Mängel zu beobachten.

Was ist zu tun?
Der Vorstand der AOK wird durch aktives Handeln deutlich machen müssen, daß von ihm erlassene Dienstanweisungen tatsächlich umgesetzt werden. Die Defizite bei der Wahrung des Sozialgeheimnisses müssen umgehend beseitigt werden. Wenn hierbei Kosten entstehen, sollten sie als in der Vergangenheit eingesparte Aufwendungen und nicht als „Mehrkosten durch den Datenschutz" angesehen werden.

4.7.3 Sozialbehörden künftig Außenstellen der Polizei?

Lange Zeit galt das deutsche Sozialgeheimnis als vorbildlich. Seit Jahren wird es aber immer mehr eingeschränkt. Den Gipfel bildet eine Gesetzesänderung, die von der Öffentlichkeit fast nicht bemerkt, in einem völlig sachfremden Gesetz, nämlich dem „Ersten Gesetz zur Änderung des Medizinproduktgesetz", versteckt wurde und die die Sozialbehörden zu Außenstellen der Polizei macht.

Bislang durften die Sozialämter und andere Sozialleistungsträger an Polizei, Staatsanwaltschaft, Gerichte und andere Behörden nur Namen, Vornamen, Geburtsdatum, Geburtsort, Anschrift sowie Name und Anschrift des Arbeitgebers übermitteln. Dies war manchen deshalb ein Dorn im Auge, weil der **„derzeitige Aufenthaltsort"** nicht zum Datenkatalog gehörte. Die Polizei konnte also nicht einfach die Namen von Gesuchten beim Sozialamt hinterlassen, um sich bei deren Auftauchen anrufen zu lassen und diese vernehmen oder festnehmen zu können. Dies war nur bei Verbrechen und sonstigen Straftaten von erheblicher Bedeutung mit **richterlicher Anordnung** und bei Sozialleistungsbetrug möglich.

Diese Rechtslage führte zu **aufgebauschten Schlagzeilen** wie: „Sozialdatenschutz ist Täterschutz". Über die Frage, ob jemand Sozialhilfe bekommen darf, nach dem zur gleichen Zeit die Polizei fahndet, kann man durchaus geteilter Meinung sein. Auch über die Reichweite des Richtervorbehalts läßt sich diskutieren. Die nunmehr ohne öffentliche Diskussion verabschiedete Einschränkung des Sozialgeheimnisses geht aber weit über das Akzeptable hinaus:

- Eine Begrenzung auf die mit Haftbefehl gesuchten Personen wurde nicht vorgenommen. Die **Polizei** kann sich künftig zur Erfüllung **aller ihrer Aufgaben** der Sozialämter bedienen. Auch die Suche nach einem Zeugen, die Erstellung von Bewegungsbildern im Rahmen der polizeilichen Beobachtung, der Abgleich von Fotos aus Radarfallen oder auch nur die Observation politisch Verdächtiger durch den Staatsschutz ist möglich. Sobald die Betroffenen bei einem Sozialleistungsträger auftauchen, ist die Polizei telefonisch zu benachrichtigen.
- Zur Datenübermittlung sind nicht nur Sozial- und Wohngeldämter, die Sozialleistungen bezahlen, sondern **sämtliche Sozialleistungsträger** verpflichtet. Dazu gehören z. B. die gesetzlichen Krankenkassen, die Rentenversicherungen und die Stellen, die Leistungen für Schwerbehinderte sowie zur Eingliederung Behinderter erbringen. Besonders empörend ist, daß auch die Jugendämter zur Mitfahndung herangezogen werden können, obwohl gerade diese das Vertrauen ihrer Klientel besonders brauchen.
- Die Polizei kann die genannten Stellen ein halbes Jahr lang (Verlängerung nicht ausgeschlossen) zur Fahndungshilfe nach einer gesuchten Person verpflichten. Überall bei den Sozialämtern, gesetzlichen Krankenkassen usw. können jetzt **Fahndungslisten** und -dateien entstehen. Zur Sachbearbeitung gehört dann künftig auch der Blick in die „schwarze Liste", der Gang ins

Nebenzimmer und der heimliche Anruf bei der Polizei.

Was ist zu tun?
Es muß darauf hingewirkt werden, daß Polizeibehörden, Staatsanwaltschaften und Gerichte keinen überzogenen Gebrauch von der neuen Befugnis machen. Das Vertrauensverhältnis zwischen den Erbringern von Sozialleistungen und ihrer Klientel würde sonst gefährdet.

4.7.4 Wenn das Sozialamt die Kontoauszüge sehen will

Im Rahmen der Überprüfung der Einkommensverhältnisse kann das Sozialamt von Hilfesuchenden die Vorlage von Kontoauszügen fordern. Diese dürfen aber nur in besonderen Ausnahmefällen zur Akte genommen werden. Schwärzungen durch den Antragsteller sind nicht grundsätzlich unzulässig.

Ein Antrag auf Renovierungsbeihilfe wurde vom Sozialamt wegen „fehlender Mitwirkung" abgelehnt, da der Antragsteller sich weigerte, die **Kontoauszüge** der letzten drei Monate im Original vorzulegen. Er hatte die Beträge und die dazu aufgeführten Texte einzelner Buchungen geschwärzt. Das Sozialamt konnte damit nicht mehr sämtliche Kontobewegungen einzeln nachvollziehen. Es wollte keinerlei **Schwärzungen** akzeptieren, denn nur so könne festgestellt werden, ob der Hilfesuchende etwas verschweige.

Die gesetzliche Mitwirkungspflicht verlangt von dem Hilfesuchenden, **alle für die Leistung erheblichen Tatsachen** anzugeben bzw. Nachweise zu erbringen. Wer dieser Mitwirkungspflicht nicht nachkommt, muß damit rechnen, daß die beantragte Leistung versagt wird. Daher ist es grundsätzlich zulässig, wenn die Sozialämter von einem Hilfesuchenden die Vorlage der Kontoauszüge der letzten drei bis sechs Monate fordern, wenn diese Leistungen beantragen, wenn in bestimmten Zeitabständen die persönlichen und wirtschaftlichen Verhältnisse überprüft werden sollen oder wenn konkrete Fragen zu den Einkommens- und Vermögensverhältnissen des Hilfesuchenden zu klären sind. Sozialämter müssen aber nicht aus Prinzip „alles" wissen.

Unzulässig, weil unverhältnismäßig ist es beispielsweise, von vornherein und ausnahmslos das Schwärzen einzelner Buchungen zu verbieten. Insbesondere **Soll-Buchungen** bis zu 100 DM sind in der Regel sozialhilferechtlich nicht relevant (z. B. Mitgliedsbeiträge für politische Parteien) und können geschwärzt werden. Es ist auch nicht erforderlich, die vorgelegten Kontoauszüge im Original oder in Kopie zur Akte zu nehmen und damit dauerhaft aufzubewahren. Zumeist genügt ein **Vermerk über die Einsichtnahme**. Der Hilfesuchende muß über den Zweck der Anforderung wie über sein Recht, einzelne Textpassagen zu schwärzen, informiert werden.

Um eine **einheitliche Verfahrenspraxis** in Schleswig-Holstein zu gewährleisten, erfolgte in Zusammenarbeit mit dem Sozialministerium eine Unterrichtung der

Kreise und kreisfreien Städte, eine Bekanntmachung im Amtsblatt Schleswig-Holstein und deren Veröffentlichung im Internet unter:



www.schleswig-holstein.datenschutz.de
(Rubrik: Informationen speziell für Behörden)

Was ist zu tun?
Sozialämter müssen die Hilfebedürftigkeit von Antragstellern überprüfen, bei der Anforderung und Auswertung aber Augenmaß bewahren.

4.7.5 Vermieterbescheinigungen für Wohngeldanträge

Mit Vermieterbescheinigungen dürfen nur die nach dem Wohngeldgesetz zur Feststellung des Wohngeldanspruches erforderlichen Daten abgefragt werden. Kann dem Antragsteller aus einem wichtigen Grund die Verwendung eines Vordruckes nicht zugemutet werden, so kann er die erforderlichen Angaben anderweitig belegen.

Eine Wohngeldstelle verlangte grundsätzlich per **Formular** von den Antragstellern die Vorlage einer vom Vermieter unterschriebenen „Vermieterbescheinigung". In dieser Vermieterbescheinigung wurde u. a. nach Mietrückständen gefragt. Eine Petentin stellte nun in Frage, ob die Angabe von Mietrückständen für die Gewährung von Wohngeld überhaupt erforderlich ist und ob es nicht möglich sei, die erforderlichen Angaben so nachzuweisen, daß der Vermieter nicht über die Wohngeldbedürftigkeit informiert wird.

Das Ministerium für Frauen, Jugend, Wohnungs- und Städtebau des Landes kam ebenso wie wir zu dem Ergebnis, daß die Wohngeldstelle von der Anforderung der vom Vermieter zu unterschreibenden **Vermieterbescheinigung** absehen kann, wenn die Verwendung dieses Vordruckes den Betroffenen nicht zugemutet werden kann. In diesem Fall sind die erforderlichen Angaben anderweitig nachzuweisen, z. B. durch Vorlage des Mietvertrags, von Bescheinigungen der Versorgungsbetriebe oder von amtlichen Bestätigungen.

Die Angabe von bestehenden **Mietrückständen** ist für die Feststellung eines Wohngeldanspruches grundsätzlich nicht erforderlich. Nur in Ausnahmefällen, z. B. wenn die Zahlung direkt an den Vermieter erfolgen soll, weil das Wohngeld nicht zur Zahlung der Miete verwendet wird, kann etwas anderes gelten. Die betreffende Wohngeldstelle hat zwischenzeitlich den **Vordruck** „Vermieterbescheinigung" entsprechend **geändert** und will die Antragsteller über deren Möglichkeiten, in anderer Form die nötigen Nachweise zu erbringen, informieren.

Was ist zu tun?
Sozialämter müssen es Antragstellern ermöglichen, Bescheinigungen, Belege u. ä. auch in einer Form beizubringen, die Dritten ihre Hilfebedürftigkeit nicht ohne Notwendigkeit offenbart.

4.7.6 Problematische Datenflüsse

Immer wieder stellen sich praktische Fragen nach Umfang und Grenzen des Sozialdatenschutzes. Hier eine Auswahl von Beispielen:

- **Bei Schulden weniger Sozialdatenschutz?**

Zur Durchsetzung von öffentlich-rechtlichen Ansprüchen von mindestens 1 000 DM im Einzelfall können von den Sozialbehörden auf Ersuchen Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen, derzeitiger und zukünftiger Aufenthalt sowie Namen und Anschriften der derzeitigen Arbeitgeber übermittelt werden, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden und wenn das Ersuchen nicht länger als sechs Monate zurückliegt.

Diese Norm im Sozialgesetzbuch eröffnet den öffentlichen Kassen eine Möglichkeit, an Informationen über ihre Schuldner zu gelangen, um die sie so mancher private Geldeintreiber beneidet. Allerdings versuchen die Landesbezirkskassen, diesen Rahmen noch etwas auszudehnen. Mit dem Hinweis, die Auskunft läge doch **im Interesse des Kostenschuldners**, weil weitere Vollstreckungsmaßnahmen vermieden werden könnten, wollte man z. B. wissen, ob ein Schuldner Sozialhilfe bezieht. Sozialamtsmitarbeiter wurden sogar um eine Beurteilung der wirtschaftlichen Verhältnisse gebeten und aufgefordert, nachzurechnen, ob Teile der Arbeitslosenhilfe bzw. des Arbeitslosengeldes gepfändet werden könnten.

Die angesprochenen Sozialämter bezweifelten zu Recht die Zulässigkeit derartiger Anfragen. Wir haben das Finanzministerium des Landes gebeten, dies gegenüber den Kassen klarzustellen.

- **Der Anruf des Wohngeld-/Sozialamtes beim Arbeitgeber**

Weil ein Wohngeldantragsteller keine vollständigen Verdienstbescheinigungen beibrachte, rief der Sachbearbeiter direkt bei dem Steuerbüro des Arbeitgebers an, um die noch fehlenden Angaben zu erfragen. Zwei Wochen nach dem Anruf hatte der Bürger seinen Wohngeldbescheid. Er war allerdings von dieser „unbürokratischen Hilfe" wenig begeistert und sah sich unangenehmen Fragen seines Arbeitgebers ausgesetzt.

Er hatte Recht. Auch wenn der Mitarbeiter des Wohngeldamtes die Antragsbearbeitung nur beschleunigen wollte, so mußte er doch den **Grundsatz der vorrangigen Datenerhebung bei dem Betroffenen** beachten. Dem obliegt die Pflicht, die für die Leistung erheblichen Tatsachen anzugeben bzw. die erforderlichen Nachweise zu erbringen. Kommt er dieser nicht fristgemäß nach, so kann die beantragte Leistung ganz oder teilweise versagt werden. Um bei dem Arbeitgeber des Antragstellers Daten zu erfragen, hätte der Mitarbeiter des Wohngeldamtes die Einwilligung des Betroffenen einholen müssen.

In einem anderen Fall hatte ein Sozialamt eine Hilfeempfängerin aufgefordert, innerhalb von vierzehn Tagen einen Arbeitsvertrag vorzulegen bzw. Angaben über die Art der ausgeübten Tätigkeit zu machen. Ohne zu warten, erkundigte er sich aber bereits drei Tage später **telefonisch** bei dem vermeintlichen **Arbeitgeber**. Der Sachbearbeiter war der Meinung, er habe keine besonders schützenswerten Daten übermittelt. Die Hilfeempfängerin war hierüber empört. Erst durch den Anruf des Sozialamtes hatte der Arbeitgeber nämlich von ihrer problematischen sozialen Lage erfahren – für sie ein denkbar schlechter Neueinstieg ins Berufsleben.

- **Die Amtsarztdiagnose im Sozialamt**

Zu den Aufgaben der Kreisgesundheitsämter gehört es, durch amtsärztliche Untersuchungen für Sozialämter festzustellen, ob Hilfeempfänger arbeits- oder berufsunfähig sind oder ob aus gesundheitlichen Gründen ein Anspruch auf Eingliederungshilfen besteht. Strittig ist häufig, ob die Sozialämter die **vollständige Diagnose** oder nur das Ergebnis einer amtsärztlichen Untersuchung erhalten dürfen. Sozialämter wollen häufig die Diagnosen der Amtsärzte „**überprüfen**", um über die beantragten Leistungen entscheiden zu können.

Auch Amtsärzte unterliegen der **ärztlichen Schweigepflicht**. Werden sie im Rahmen des sozialhilferechtlichen Verwaltungsverfahrens als begutachtende Stelle eingeschaltet, so ergibt sich aus der Natur dieses Verfahrens eine begrenzte Übermittlungsbefugnis. Diese beschränkt sich auf das Ergebnis der amtsärztlichen Untersuchung, das ausreicht, um über den Antrag entscheiden zu können. Die Kenntnis der vollständigen Diagnose ist nur in Ausnahmefällen erforderlich. Der Hilfesuchende selbst kann allerdings die vollständige Diagnose jederzeit beim Amtsarzt erfragen bzw. einsehen.

- **Wenn Wohnungsamt und Sozialamt enger zusammenarbeiten als erlaubt**

Eine Sozialhilfeempfängerin ließ sich bei ihrem Wohnungsamt in die Liste der Wohnungssuchenden eintragen. Sie war nicht vom Sozialamt aufgefordert worden, sich um kostengünstigeren Wohnraum zu bemühen. Nach der Trennung von ihrem Mann war ihr jedoch die Wohnung zu groß und zu teuer erschienen. Sie wollte also aus eigenem Antrieb Kosten sparen. Das Wohnungsamt bot ihr auch zwei günstige Wohnungen an. Nach einigen Überlegungen lehnte die Hilfeempfängerin jedoch aus persönlichen Gründen diese Angebote ab. Das Wohnungsamt akzeptierte die Ablehnungsgründe nicht und schloß die Hilfeempfängerin für sechs Monate von einer weiteren Wohnungsvermittlung aus. Die **Durchschrift** dieses Bescheids ging **an das Sozialamt**. Das Wohnungsamt meinte, es müsse das Sozialamt immer informieren, wenn der Umzug in eine billigere Wohnung abgelehnt wird. Die Hilfeempfängerin befürchtete nun Schwierigkeiten mit dem Sozialamt.

Das Sozialamt benötigte die Angaben über die Ablehnung der Wohnungsangebote nicht. Die Hilfeempfängerin bewohnte eine angemessene Wohnung und war nicht zu einem Umzug aufgefordert worden. Auch gehört es nicht zu den Aufgaben des

Wohnungsamtes, **pauschal** Daten an das Sozialamt zu übermitteln. Die Weitergabe des Bescheides vom Wohnungsamt an das Sozialamt war somit unzulässig. Auf Nachfrage erklärte das Wohnungsamt, die Datenübermittlung sei versehentlich erfolgt. Für dieses Versehen entschuldigte sich das Wohnungsamt bei der Hilfeempfängerin. Das Sozialamt hat die Durchschrift des Bescheides zwischenzeitlich vernichtet.

- **„Schwarze Akte" im Sozialamt**

Eine Sozialhilfeempfängerin wußte nicht mehr weiter. Sie berichtete uns, daß sie mit dem für sie bislang zuständigen Sozialamt stets große Schwierigkeiten hatte. Sie hoffte nach einem Umzug also auf einen Neubeginn in dem nunmehr zuständigen Sozialamt. Um so größer war jedoch ihr Erstaunen, als sie in der neuen Gemeinde die gleichen Schwierigkeiten bekam. Schon bald merkte sie, daß man dort über Informationen verfügte, die man nur von dem zuvor zuständigen Sozialamt hatte erfahren können und die zudem in keinem Zusammenhang mit der Sozialhilfegewährung standen. So war sogar bekannt, wo sie vor drei Jahren Urlaub gemacht hatte.

Anläßlich eines Ortstermines mußten wir Erstaunliches feststellen. Die Mitarbeiterin des Sozialamtes hatte **die komplette Sozialhilfeakte** der zuvor zuständigen Gemeinde angefordert und vollständig – ca. 600 Seiten – kopiert. Auf die Nachfrage, ob dieses denn erforderlich sei, bekamen wir die Antwort: „Naja, eigentlich brauchen wir nicht alle Seiten, aber die alte Gemeinde bzw. der Kreis hat uns vorgewarnt, daß es sich hier um einen besonders schwierigen Fall handeln würde. Wir sollten genau aufpassen, was wir sagen, da sich die Hilfeempfängerin alles merkt und dann das Sozialamt schlecht macht." Unter den Kopien befanden sich ärztliche Atteste, Gutachten des Medizinischen Dienstes, ein Scheidungsurteil, Unterhaltsvereinbarungen, alte Mietverträge und Stellungnahmen des Diakonischen Werkes aus den letzten Jahren. Besonders problematisch war die Aufbewahrung der Kopien in einem unbeschrifteten Extraordner, der in einem offenen Regal im Büro der Sachbearbeiterin stand.

Das Führen der „**schwarzen Akte**" stellte in mehrfacher Hinsicht einen Verstoß gegen den Sozialhilfedatenschutz dar. Die Übermittlung einer vollständigen Akte zwischen Trägern der Sozialhilfe ist nur dann zulässig, wenn alle in dieser Sozialhilfeakte enthaltenen Sozialdaten für die Sozialhilfegewährung bei dem nunmehr zuständigen Sozialamt erforderlich sind. Davon konnte hier keine Rede sein. Zudem ist auch die Speicherung von Sozialdaten nur im Rahmen der Erforderlichkeit zulässig. Auch dies war nicht der Fall. Alle Sozialdaten, die zu Recht gespeichert werden, sind Gegenstand des Verwaltungsverfahrens. Sie unterliegen dem Sozialgeheimnis, der Betroffenen ist auf Antrag Auskunft zu erteilen. Eine „schwarze Akte" vorzuhalten, von der die Betroffene nichts wußte, die aber bei Bedarf gegen sie verwendet wurde, stellte einen schweren Datenschutzverstoß dar. Auf unsere Beanstandung hin wurde die Akte vernichtet.



4.8 Schutz des Patientengeheimnisses

4.8.1 Gesetzgebungsvorhaben

Das Ministerium für Arbeit, Gesundheit und Soziales hat uns im Berichtszeitraum den Entwurf eines Gesundheitsdienstgesetzes sowie eines Psychisch-Kranken-Gesetzes zukommen lassen. In beiden Fällen wurde auf besondere datenschutzrechtliche Bestimmungen verzichtet, da diese in einem **Gesundheitsdatenschutzgesetz** Aufnahme finden sollen. Eine solche Konzentration der Datenschutzregelungen im medizinischen Bereich wird von uns begrüßt, wenn damit zugleich eine Verbesserung des Schutzes der hochsensiblen medizinischen Daten erreicht wird. Seit Jahren steht das Ministerium im Wort, tätig zu werden. Ernüchternd war deshalb die aktuelle Mitteilung, daß in absehbarer Zeit die personellen und fachlichen Ressourcen für dieses Gesetzgebungswerk nicht zur Verfügung stünden. Zwar signalisierte das Ministerium erneut seine Absicht, inhaltlich einen „Großen Wurf" zu versuchen. Es sollen nicht nur das öffentliche, sondern auch das private Gesundheitswesen erfaßt und der Einsatz neuer Medien (z. B. Vernetzung, Chipkarten, digitale Krankenakte) einbezogen werden. Allein, die schönsten Absichtsbekundungen sind nichts wert, wenn ihnen keine Taten folgen.

Im **Psychisch-Kranken-Gesetz** fehlen nach unserer Auffassung Klarstellungen, die die medizinische Selbstbestimmung absichern (Einholung von Zustimmungen, Ermöglichung von Gegendarstellungen, Transparenz für die Betroffenen). Dieses Recht auf Selbstbestimmung steht auch psychisch Kranken zu. Werden deshalb Daten bei der Inanspruchnahme freiwilliger psychiatrischer Hilfen preisgegeben, so dürfen diese nicht ohne weiteres für Zwangsmaßnahmen, z. B. für eine zwangsweise Unterbringung genutzt werden.

Durch das Ende 1999 außer Kraft tretende Bundes-**Krebsregistergesetz** werden die Länder verpflichtet, flächendeckend bevölkerungsbezogene Register einzuführen bzw. nach Landesrecht weiterzuführen. Seit Beginn des Jahres 1998 ist ein solches Register in Schleswig-Holstein in Betrieb (vgl. 19. TB, Tz. 4.8.1). Um dieses nach Auslaufen des Bundesgesetzes auf eine Rechtsgrundlage zu stellen, wurde ein Gesetzentwurf des Ministeriums für Arbeit, Gesundheit und Soziales vorgelegt. Das bisherige schleswig-holsteinische Modell wird mit kleinen Modifikationen beibehalten werden. Wir bleiben im Interesse des Datenschutzes sowohl im Rahmen der Gesetzgebung wie auch beim Betrieb des Registers und bei der Durchführung von Forschungsprojekten mit Registerdaten einbezogen.

4.8.2 Neufassung der Ärztlichen Berufsordnung

Die Ärztekammer möchte ihre Berufsordnung entsprechend einer bundesweiten Musterordnung überarbeiten. Damit soll das Standesrecht den neuesten rechtlichen und technischen Entwicklungen angepaßt werden. Aus der Sicht der Patienten besteht Nachbesserungsbedarf.

Gegen die geplante Übernahme der bundesweiten Musterordnung durch die Ärztekammer Schleswig-Holstein mußten wir Bedenken anmelden. Dies betraf

zunächst die Einsicht der Patientinnen und Patienten in Akten, die bezüglich Teilen, „welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten", ausgeschlossen werden soll. Damit knüpft die Regelung an eine alte Rechtsprechung des Bundesgerichtshofes (BGH) aus den 80er Jahren an, obwohl inzwischen neuere patientenfreundlichere Urteile vorliegen. Daraus ergibt sich, daß **Akteneinsicht** für Patienten kein Gnadenakt ist, sondern Bestandteil medizinischer Selbstbestimmung. Die vorgesehene Ausnahme vom Akteneinsichtsrecht der Patienten ist deshalb viel zu weit formuliert. Leider war die Ärztekammer nicht bereit, ihren Entwurf entsprechend zu verbessern.

Dies gilt auch für die Regelung des Umgangs mit dem Patientenarchiv im Fall einer ärztlichen **Praxisaufgabe bzw. -übergabe**. Mit der vorgesehenen Anordnung, die Patientenakten in diesen Fällen „in gehörige Obhut" zu geben, sind die strengen Regeln der jüngsten Rechtsprechung des BGH nicht ausreichend berücksichtigt. Danach muß der Wille der Betroffenen beim Übergang der Verantwortung über die Patientenakten erkundet und berücksichtigt werden. Dies bedeutet, daß in jedem Fall zuerst versucht werden muß, die Einwilligung der Patienten zu erlangen.

Die Ärztekammer wie auch das Gesundheitsministerium erkannten die von uns aufgezeigten Probleme an. Dennoch war es nicht möglich, klarere und patientenfreundlichere Regelungen durchzusetzen. Wir werden der Ärztekammer präzisierende Erläuterungen vorlegen, damit negative Auswirkungen auf das informationelle Selbstbestimmungsrecht der Patienten soweit wie möglich vermieden werden.

Was ist zu tun?
Die Schwächen der neuen Berufsordnung sind im Rahmen der Auslegung und Anwendung auszugleichen.

4.8.3 Patientenakten für die Kassenzahnärztliche Vereinigung?

Bei der notwendigen Kontrolle der Abrechnung medizinischer Leistungen muß Rücksicht auf das Patientengeheimnis genommen werden. Konflikte lassen sich auf Dauer nur durch eine sachgerechte Datenorganisation bei den Ärzten vermeiden.

Geld ist im Gesundheitswesen zum zentralen Konfliktanlaß geworden: Wer muß welche medizinischen Kosten tragen? Wo bestehen Einsparpotentiale? Welche Leistungen sind überflüssig oder überteuert? Bei der **Abrechnung medizinischer Leistungen** werden naturgemäß personenbezogene Daten offenbart, die dem besonderen Schutz der ärztlichen Schweigepflicht unterliegen. Hier gilt es Lösungen zu finden, die das notwendige Maß an Nachprüfung von Abrechnungen ebenso wie das besondere Vertrauensverhältnis zwischen Arzt und Patient berücksichtigen. Es ist daher kein Wunder, daß auch die Datenschutzbeauftragten in die Diskussionen über die Finanzierung des Gesundheitssystems hineingezogen werden.

Eine Zahnärztin beschwerte sich darüber, daß sie von der Kassenzahnärztlichen Vereinigung (KZV) aufgefordert worden war, „zur sachlich-rechnerischen Überprüfung und ggf. Berichtigung Ihrer kons.-chir. Abrechnungen II/96 und III/96" u. a. die Kopien von 134 Patientenkarteikarten vorzulegen. Insgesamt sollte sie Unterlagen über 262 Personen einreichen.

Tatsächlich sieht das Sozialgesetzbuch V zur Rechnungskontrolle die Vorlagepflicht von Befunden bei der Kassenärztlichen Vereinigung vor. Anhand der vollständigen Beschreibung der erbrachten Leistung sollen **Plausibilitätskontrollen** ermöglicht werden. Genügen diese Prüfungen nicht, so sieht das Gesetz eine Wirtschaftlichkeitsprüfung oder eine Kontrolle durch den Medizinischen Dienst vor. Das Vorlegen vollständiger Karteikarten an die KZV geht aber weit über das Erforderliche hinaus, da hierauf auch andere Angaben als Befunde sowie Angaben über Behandlungen außerhalb des Überprüfungszeitraumes enthalten sind. So teilte die Petentin mit, daß unter den von ihr Behandelten auch ein Mitarbeiter der KZV sei. Bei Vorlage der gesamten Karteikarte hätte die KZV hochsensible Informationen über einen ihrer eigenen Bediensteten erfahren können.

Obwohl eine solch weitgehende Datenoffenbarung unzulässig ist und für die Ärztin diese zu einer strafrechtlich relevanten Verletzung ihrer Schweigepflicht geführt hätte, sah sich die KZV nicht gehindert, eine Entscheidung „nach Aktenlage" anzukündigen, sollten nicht endlich die Unterlagen vorlegt werden. Die Zahnärztin erklärte sich bereit, für eine umfassende Abrechnungskontrolle mit all ihren Karteikarten in die KZV zu kommen, um dann auf Nachfrage gezielt Einblick in ihre Unterlagen zu geben. Dies war aber für die KZV **„aus verwaltungspraktischen Erwägungen"** nicht gangbar. Die von der KZV vorgeschlagene Schwärzung aller überschüssigen Informationen auf den Karteikarten wollte wiederum die Petentin wegen des damit verbundenen unverhältnismäßigen Aufwandes nicht akzeptieren. Bei Redaktionsschluß war die Sache noch nicht entschieden.

Was ist zu tun?
Die Ärztinnen und Ärzte sollten angehalten werden, ihre Patientenunterlagen von vornherein so zu organisieren, daß die absehbar abrechnungsrelevanten Angaben problemlos von den besonders sensiblen medizinischen Zusatzinformationen zu trennen sind.

4.9 Schule, Hochschule, Wissenschaft

4.9.1 Datenschutzverordnung als „Blockwartsystem"?

Immer mehr Lehrer verarbeiten mit privaten PC Schülerdaten im häuslichen Bereich. Auch nachdem das gesetzliche Verbot der Nutzung von Privat-PC für dienstliche Zwecke gelockert wurde, schmecken einigen Lehrern die Rahmenbedingungen hierfür nicht.

1. Szenario:

Man stelle sich vor: Ein Finanzamt bittet aus Platzmangel einen Teil seiner Mitarbeiter, die Steuererklärungen der Steuerpflichtigen zu Hause zu bearbeiten. Jeder Beamte kann seine Arbeit so verrichten, wie er möchte, da keine besonderen Regelungen erlassen werden. Einige bearbeiten nun die Steuererklärungen im häuslichen Wohnzimmer. Sensible Unterlagen mit Angaben z. B. zu Unterhaltsleistungen an Dritte, Nachweisen für erhöhte Aufwendungen wegen Behinderung usw. liegen für andere Familienmitglieder einsehbar herum. Andere wiederum, die ein eigenes Arbeitszimmer haben, schließen die Unterlagen nicht weg, da sich das Zimmer ja in der eigenen Wohnung befindet. Für Mißtrauen gegenüber den eigenen Familienangehörigen besteht aus ihrer Sicht kein Anlaß. Manche Mitarbeiter benutzen für die Sachbearbeitung ihren eigenen PC, der allerdings auch von anderen Familienmitgliedern genutzt wird. Ein anderer betreibt eine Mailbox auf seinem Computer, der an das Internet angeschlossen ist. Die Steuerdaten der Bürger im Rechner sind, weil der Finanzamtsmitarbeiter dies nicht für nötig hält („was soll da schon passieren") und ihn auch keine Dienstvorschrift dazu anhält, vor dem Zugriff virtueller Besucher nicht geschützt. Möglicherweise studieren und kopieren fremde Hacker interessiert die Steuererklärung anderer Leute oder machen sich einen Spaß daraus, die Zahlen zu manipulieren.

Wer würde in Kenntnis dieser Zustände noch Vertrauen in die ordnungsgemäße und vertrauliche Verarbeitung seiner Steuerdaten durch die Finanzverwaltung haben?

2. Szenario:

Man stelle sich vor: Den Schulleitungen wird im Rahmen der Dezentralisierung und Verschlankung die Personalaktenführung übertragen. Manche Schulleiter schaffen es nicht, während des laufenden Schulbetriebes auch noch die Lehrereinsatzplanung und den „Personalverwaltungskram" zu erledigen. Deshalb nehmen sie Personalakten zu sich nach Hause. Den Lehrereinsatz verwalten sie mit einem auf dem Privat-PC installierten Programm. Zwecks reibungsloser Planung werden die Urlaubs-, Lehrgangs- und Krankheitsfehlzeiten gespeichert. Für die Beurteilung der Lehrkräfte werden eigene Dateien angelegt. Auf Einwände einzelner Lehrer würden die Schulleiter antworten, als Beamte seien sie doch zur Verschwiegenheit verpflichtet, da könne man ihnen schon vertrauen. Sollte die vorgesetzte Stelle auf die Idee kommen, sich die Sache einmal vor Ort anzusehen, würden die Schulleiter die Unverletzlichkeit ihrer Wohnung geltend machen.

Was wohl die Personalräte dazu sagen würden?

Die Szenarien mögen konstruiert klingen. So oder so ähnlich argumentieren manche Lehrer aber, seit das Bildungsministerium die Nutzung privateigener PC für dienstliche Zwecke unter bestimmten Voraussetzungen zugelassen hat. In einigen Eingaben wurde geltend gemacht, die Datensicherungsregelungen zeugten von **Mißtrauen** gegenüber den Lehrern und ihre Einhaltung erfordere zuviel Aufwand. Als **rechtstreue Beamte** bräuchten sie nicht mit Regeln zur Datensicherheit und Kontrollen überzogen werden. Die geforderte Einwilligung in etwaige Kontrollen durch Schulleitung oder den Datenschutzbeauftragten komme einer Preisgabe der häuslichen Privatsphäre gleich. Ein Lehrer sprach gar von „Kontrollstaat" und „Denunziantentum"; er fühle sich an das „Blockwartsystem" vergangener Zeiten erinnert.

Im Gegensatz dazu haben insbesondere **Informatiklehrer** mit der neuen Regelung keine Probleme. Bei der Vorstellung und Erläuterung der Datenschutzverordnung Schule zeigte sich, daß es für sie eine Selbstverständlichkeit ist, die Arbeit mit Schülerdaten am privaten PC als Datenverarbeitung durch eine öffentliche Stelle zu verstehen, die gewisse Sicherheitsstandards und Kontrollmöglichkeiten unumgänglich macht. Tatsächlich geht es im wesentlichen um das kleine Einmaleins der Datensicherheit. Denn auch Daten über Schüler und ihre Eltern können sehr sensibel sein. Sie unterliegen dem gleichen Schutz wie andere bei der Verwaltung verarbeitete Daten über Bürgerinnen und Bürger. Für diese Daten trägt die Schule auch dann die Verantwortung, wenn die Verarbeitung zu Hause am privaten PC stattfindet. Sie gehören nicht zur „privaten Verfügungsmasse" der Lehrer.



Was ist zu tun?
Lehrer, die ihren häuslichen PC für dienstliche Zwecke nutzen, sollten akzeptieren, daß dies keine reine Privatangelegenheit ist.

4.9.2 Schulabgängeradressen für Werbezwecke gesucht!

Unternehmen versuchen mit Hilfe von „Wettbewerben", „Tests" oder „Analysen" an Adreßmaterial von Schülern zu gelangen, um anschließend gezielte Werbemaßnahmen zu starten. Auch die gesetzlichen Krankenkassen mischen mit.

Von Schulen, Eltern sowie von betroffenen Schülerinnen und Schülern werden wir immer wieder auf die fragwürdigen Praktiken z. B. von Krankenversicherungen hingewiesen, mit denen sie an Adreßmaterial sowie zusätzliche Informationen von Schulabgängern zu gelangen versuchen. Dies geschieht mit Hilfe von Wettbewerben oder durch das Angebot von Berufsbildanalysen. So verteilte eine gesetzliche Krankenkasse im Rahmen ihrer gesundheitlichen Aufklärung in der Schule Karten für die Teilnahme an einem **Quiz** und beschaffte sich so Namen und Anschriften der Schülerinnen und Schüler, um diese daraufhin gezielt mit Werbung anzusprechen.

Eine Bausparkasse bot über ein mit ihr verbundenes Institut einen **Berufsinteressentest** an, durch den die Schülerinnen und Schüler Anregungen für die zukünftige Studien- oder Berufswahl erhalten sollten. Wäre dieser Test, wie zunächst geplant, personenbezogen durchgeführt worden, so hätte die Bausparkasse über die ausgefüllten Fragebögen nicht nur Namen und Anschriften der heranwachsenden jungen Menschen erhalten, sondern auch aussagefähige Persönlichkeitsbilder. Diese Informationen wären für Werbezwecke buchstäblich Gold wert gewesen; die informationelle Selbstbestimmung hätte das Nachsehen gehabt. Wir konnten erreichen, daß eine Anonymisierung der Fragebögen erfolgte.



Bei all diesen Aktionen versuchen die Firmen ganz geschickt, die **Schulleitungen** oder gar das **Bildungsministerium** als Partner zu gewinnen und sich so einen leichteren Zugang zu den Schülerinnen und Schülern zu verschaffen. Sind diese bereit, ihre Angaben freiwillig herauszugeben, so kann das im Schulgesetz verankerte Werbe- und Übermittlungsverbot umgangen werden. Wir haben das Bildungsministerium auf diese Tricks hingewiesen, das daraufhin die Schulen entsprechend unterrichtete.

Was ist zu tun?
Die Schulen sollten sorgfältig die datenschutzrechtlichen Aspekte prüfen, bevor sie Wettbewerbe, Tests etc. von Unternehmen unterstützen.

4.9.3 Studi-Chipkarten

In der Fachhochschule und der Medizinischen Universität Lübeck wurden Chipkarten als Studierendenausweise eingeführt. Weitere Hochschulen wollen folgen.

Die mit der geplanten Studi-Chipkarte verbundenen Versprechungen hinsichtlich Verwaltungsrationalisierung und Arbeitsentlastung hören sich äußerst verheißungsvoll an. Rückmeldungen, Kostenabrechnungen und Berechtigungskontrollen und noch viel mehr soll mit Chipkarten einfacher, schneller und billiger gehen. Eine eingehende Erörterung mit allen Beteiligten zeigte schnell, daß Innovationsfreude und Tatkraft allein für die Einführung von Chipkarten mit derart vielfältigen Funktionen nicht genügen. Neben einer Vielzahl technischer Fragen mußten auch rechtliche Fragen geklärt werden. Die Einführung eines **obligatorischen Studierendenausweises** in Form einer Chipkarte bedarf einer bereichsspezifischen Rechtsgrundlage. Deshalb findet in Lübeck der Chipkarteneinsatz zunächst auf freiwilliger Basis statt. Die Betroffenen sind über die Funktionsweise und die Zwecke sowie über die Widerrufbarkeit ihrer schriftlichen Einwilligung unterrichtet worden.

Parallel dazu arbeiteten wir an einem Regelungsvorschlag zur Änderung der **Studierenden-Datenverordnung** mit, in dem der Datensatz und die Zwecke der Anwendungen sowie die zulässigen Formen der Nutzung der Chipkarte festgelegt werden. Um die Transparenz für die Betroffenen zu gewährleisten, wurde das Auskunftsrecht betont und die Pflicht, jede Kommunikation zwischen Chipkarte

und Lesegerät erkennbar zu machen, normiert.

Was ist zu tun?
Der obligatorische Studierendenausweis als Chipkarte kann erst nach Änderung der Studierenden-Datenverordnung und nach Durchführung des Freigabeverfahrens erfolgen.

4.9.4 Was brächte ein Forschungsgeheimnis?

Das Verhältnis zwischen Wissenschaft und Datenschutz steht seit über zwanzig Jahren in der Diskussion. Von Anfang an wurde „dem Datenschutz" der Vorwurf gemacht, „die Forschung" zu behindern. Vorschläge zur Änderung des Landesdatenschutzgesetzes und zur Einführung eines Forschungsgeheimnisses könnten zur Konfliktlösung beitragen.

Zwar wurden uns derartige Pauschalvorwürfe in Schleswig-Holstein nicht vorgetragen. Gleichwohl stellen sich auch hier immer wieder Abgrenzungsfragen, in letzter Zeit häufig verbunden mit der Forderung nach einem Forschungsgeheimnis. Für Forschende sollen ein umfassendes Schweigerecht und eine Schweigepflicht gelten. Im Gegenzug sollen sie **freien Zugang** zu zumeist medizinischen, personenbezogenen Daten erhalten – eine „Lizenz zum Forschen". Derartige Vorstellungen sind mit deutschem Verfassungsrecht und europäischen Vorgaben allerdings nicht vereinbar.

Unser Vorschlag für eine **Novellierung des Landesdatenschutzgesetzes** sieht in einer Forschungsklausel aber einige wesentliche Erleichterungen für Wissenschaftler vor, insbesondere wenn diese mit anonymisierten oder pseudonymisierten Daten arbeiten wollen. Nur wenn eine solche Anonymisierug nicht möglich ist, muß versucht werden, die Einwilligung der Betroffenen einzuholen. Eine weitere Vereinfachung soll darin bestehen, daß Projektmitarbeiter des Forschungsvorhabens im Rahmen einer Personalüberlassung bei der verarbeitenden Stelle die Anonymisierung bzw. Pseudonymisierung selbst vornehmen können, wenn sie den Weisungen und der Aufsicht der speichernden Stelle unterliegen.

Diese Regelungen entbinden aber den Bundesgesetzgeber nicht, sich Gedanken zu einem dem Arztgeheimnis rechtlich nachempfundenen **Forschungsgeheimnis** zu machen. Es soll aber keine pauschale Befugnisnorm für die Forschenden darstellen, sondern vorrangig die Betroffenen schützen. Eine strafbewehrte Schweigepflicht der Forscher, verbunden mit einem Beschlagnahmeverbot, würde allerdings auch das Vertrauen zur Forschung und damit die Kooperationsbereitschaft gegenüber den Wissenschaftlern stärken.

Was ist zu tun?
Die Regelungen für den Datenschutz im Forschungsbereich sollten auf Bundesebene um ein Forschungsgeheimnis im Interesse der Bürgerinnen und Bürger erweitert werden.

4.10 Steuerverwaltung

4.10.1 Steuerdatenabrufverordnung – es grenzt an einen Schildbürgerstreich

Der Streit zwischen Behörden verhindert bisher einen einheitlichen Sicherheitsstandard beim automatisierten Abruf von Steuerdaten.

Wenn früher ein Finanzbeamter für die Bearbeitung eines Vorganges aus seinem Zuständigkeitsbereich Informationen aus einer Steuerakte einer anderen Abteilung oder eines anderen Finanzamtes benötigte, ließ er sich vom betreffenden Kollegen eine Auskunft erteilen oder forderte die Akte zur Einsichtnahme an. Die Rechtmäßigkeit eines solchen **Datenaustausches** im Hinblick auf die Wahrung des Steuergeheimnisses, das auch innerhalb der Verwaltung gilt, konnte wegen des aktiven Handelns von mindestens zwei Personen leicht überprüft werden.

Als im Zeichen der Automatisierung in den Finanzämtern die Steuerdaten zunehmend in Computerdatenbanken gespeichert wurden, entstand der Wunsch, die erforderlichen Informationen auch direkt aus den **EDV-Systemen** abrufen zu können. Dies hat der Gesetzgeber im Jahre 1985 durch eine Änderung der Abgabenordnung gestattet, aber zur Vermeidung von Datenmißbräuchen (es entfiel ja die Kontrolle der Rechtmäßigkeit durch den Kollegen, der die Daten „rauszurücken" hatte) bestimmt, daß der Bundesfinanzminister in einer Rechtsverordnung festlegen kann, „welche technischen und organisatorischen Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind".

Von der Möglichkeit des automatisierten Datenabrufes haben die Finanzämter umgehend Gebrauch gemacht. Auf die **sicherheitstechnischen Rahmenbedingungen** konnten sich der Bund, die Länder und die Kommunen, die z. B. für die Grund- und Gewerbesteuern zuständig sind, jedoch im Verlaufe von 13 Jahren (!) nicht einigen. Als sich vor etwa zwei Jahren Bund und Länder nach der Diskussion von ca. zwei Dutzend Entwürfen endlich auf ein Regelwerk verständigt hatten, das im wesentlichen auch den datenschutzrechtlichen Belangen entsprach, bekamen sie Sperrfeuer von den kommunalen Verbänden, weil denen das technische Sicherheitsniveau zu hoch erschien. Nach einer Phase der Ratlosigkeit gelang im abgelaufenen Jahr ein wahrer Schildbürgerstreich. Anstelle einer Rechtsverordnung erließ der Bundesfinanzminister den unveränderten Text als bundeseinheitliche Verwaltungsanweisung, die allerdings nur für die Finanzämter, nicht aber für die kommunalen Steuerbehörden verbindlich war.

Kaum war dies geschehen, signalisierten die Kommunen, sie könnten mit diesen Regelungen wahrscheinlich doch leben. Noch in diesem Jahr wird deshalb auf höchster Ebene eine neue Verhandlungsrunde beginnen. Man darf gespannt sein, wann die Verwaltung sich endlich bereit findet, einen Auftrag des Gesetzgebers, der ihr im Jahr 1985 erteilt wurde, zu erfüllen.

Was ist zu tun?
Die Finanzminister sollten ein Machtwort sprechen, die Verordnung beschließen und alle Steuerbehörden anweisen, endlich die Sicherheitsvorschriften zu beachten, die schon vor 13 Jahren als sinnvoll angesehen waren.

4.10.2 Registrierung von Barzahlern als Druckmittel

Die Finanzämter haben einen Anspruch darauf, Einblick in alle Buchführungsbelege zu erhalten. Dabei dürfen sie auch Daten über Dritte (Kunden, Lieferanten, Mitarbeiter) zur Kenntnis nehmen. Sie können aber nicht verlangen, daß die Identität von „Barzahlern" nur deshalb ermittelt wird, um die Steuerpflichtigen zu mehr Steuerehrlichkeit zu bewegen.

Die Finanzämter haben es wahrlich nicht leicht: Der Finanzminister drängt sie, sehr genau hinzusehen und möglichst jeden auch noch so kleinen Steuerbetrag zu kassieren. Die Steuerpflichtigen bemühen sich dagegen manchmal redlich, manchmal unredlich, den Beamten weis zu machen, daß von ihnen getätigte Geschäfte gar keine Geschäfte waren und somit auch keine Steuer fällig werden könne. Bei besonders hartleibigen Steuerpflichtigen greifen deshalb Steuerbeamte das eine oder andere Mal zu Mitteln, die mit dem geltenden Recht nur schwer vereinbar sind.

Um vermeintlichen unerlaubten Steuertricksereien auf die Spur zu kommen, verpflichtet man die „verdächtigen" Steuerpflichtigen gerne und in zunehmendem Maße zu besonders umfangreichen Aufzeichnungen. So sollte z. B. ein Verein die Identität auch von solchen Spendern feststellen, die eine **Barspende** geleistet hatten und keinen Wert auf eine Spendenbescheinigung legten. Dem Geschäftsführer wurde erklärt, hierzu sei er verpflichtet, weil der Verdacht von Unregelmäßigkeiten bei der Vereinsfinanzierung bestehe und deshalb die Gemeinnützigkeit zu überprüfen sei. Die Frage, ob deshalb der Verein auf anonyme Spenden verzichten müßte, und wer einen Spender (z. B. bei Straßensammlungen) zwingen könne, seinen Namen preiszugeben, konnte nicht beantwortet werden. Wir haben dem Geschäftsführer mitgeteilt, daß er nach unserer Auffassung dem Ansinnen des Finanzamtes nicht nachkommen muß. Es hat die Sache offenbar auf sich beruhen lassen. In einem anderen Fall sollte der Vermieter von Ferienwohnungen auch dann die **Identität von Mietern** in der Buchführung vermerken, wenn die Gäste ihre Miete bar bezahlten. Auch hiergegen hat sich der Steuerpflichtige erfolgreich verwahrt.

Für diese und vergleichbare Fälle (vgl. z. B. die angebliche Pflicht der Apotheker, die Kundennamen im Fahrtenbuch zu vermerken, wenn die bereits bezahlten Arzneien frei Haus geliefert werden, 19. TB, Tz. 4.10.3) gelten folgende Kontrollfragen: Wozu will das Finanzamt die Daten verwenden? Will es z. B. alle Spender fragen, ob sie tatsächlich gespendet, oder alle Mieter, ob sie tatsächlich dort übernachtet haben? Wie ist zu entscheiden, wenn sich herausstellt, daß die Identitäten nicht stimmen? Trägt dann der Steuerpflichtige die Verantwortung und muß mehr Steuern zahlen?

Was ist zu tun?
Die Finanzämter müssen zur Kenntnis nehmen, daß kein Bürger verpflichtet ist, bei Bargeschäften seine Identität preiszugeben, es sei denn, es bestehen ausdrückliche gesetzliche Regelungen, wie z. B. im Geldwäschegesetz. Hieraus

folgt, daß die Aufforderung zur Erfassung von Kundendaten kein Druckmittel gegenüber Steuerpflichtigen sein kann.

4.10.3 Restrisiken beim Fax-Verkehr

Bei der Verwendung von Fensterbriefumschlägen kommt es selten vor, daß ein Schriftstück beim falschen Empfänger landet. Seit allerdings sogar Steuerdaten von den Finanzämtern per Fax versandt werden, reicht ein Tippfehler und schon ist das Steuergeheimnis verletzt.

Da staunte Herr X nicht schlecht, als sein Fax-Gerät plötzlich die Mitteilung eines Finanzamtes ausspuckte, sein beantragter Zahlungsaufschub für die xxx-Steuer in Höhe von xxx DM werde ihm hiermit gewährt. Er hatte nämlich gar keine Stundung beantragt. Bei genauerem Hinsehen stellte er fest, daß dieses **Fax** von einem **Finanzamt** am anderen Ende Schleswig-Holsteins stammte und gar nicht für ihn bestimmt war. Es war nur deshalb auf seinem Gerät gelandet, weil dem Absender in die Ortskennzahl eine falsche Ziffer gerutscht war. Nun wußte er, weil ja der richtige Name in dem Schreiben vermerkt war, wer die Steuerschulden und obendrein Zahlungsschwierigkeiten hatte.

Daß ein Fehler vorlag, wurde vom Finanzamt nicht bestritten. Wäre er aber zu verhindern gewesen? Die Untersuchung ergab folgendes: Mit großer Akribie hatte die Oberfinanzdirektion im Jahre 1989 die Telefaxnutzung durch die Finanzämter geregelt. Bezeichnend ist allerdings für die „Motivlage" das Zitat aus einer Dienstanweisung: „Wegen der Portoerhöhungen der Bundespost und des Preisverfalls bei den Telefaxgeräten ist es nunmehr **wirtschaftlich** und **zweckmäßig**, die Dienststellen der Steuerverwaltung mit Faxgeräten auszustatten." Es folgen dann auf ca. 20 Seiten vielfältige Handlungsanweisungen wie z. B.

- liegt die Fax-Einverständniserklärung des Adressaten vor?
- Steuerbescheide nicht per Fax bekannt geben!
- sensible Schriftstücke nur nach Absprache mit dem Beteiligten faxen!
- Vorblatt zur Absender-/Empfängeridentifikation oder Vollständigkeitskontrolle erforderlich?
- Fax-Nummer des Adressaten noch gültig?
- Fax-Nummer richtig eingegeben?
- Sendeprotokoll prüfen und dem Vorgang beifügen!

Trotz all dieser Vorsichtsmaßnahmen, der Fall zeigt drei Dinge:

Ein Tippfehler genügt, und schon ist das Steuergeheimnis verletzt. Der Schaden ist nicht rückgängig zu machen. Das (Rest)risiko wird zunehmend größer, da sich hinter immer mehr Telefonnummern auch Faxgeräte „verstecken".

Der Verlust der Vertraulichkeit darf nicht der Preis für die vorgenannten Zweckmäßigkeits- und Wirtschaftlichkeitsüberlegungen sein.

Was ist zu tun?
Künftig sollten Textdokumente mit steuerlichen Inhalten nur dann per Fax versandt werden, wenn eine außergewöhnliche Eilbedürftigkeit besteht und die Steuerpflichtigen ausdrücklich darum gebeten haben. In diesen seltenen Ausnahmefällen muß von den Mitarbeitern eine entsprechende Sorgfalt bei der Adressierung erwartet werden. Sie sollten über die Folgen von Fahrlässigkeiten aufgeklärt werden.

4.10.4 Wahrung des Steuergeheimnisses – in erster Linie eine Frage der Haushaltsmittel?

Wer tagtäglich mit „hochsensiblen" Steuerdaten umgeht, verliert offenbar leicht das Gefühl für das erforderliche und angemessene Sicherheitsniveau. Anders ist nicht zu erklären, warum gravierende Sicherheitsmängel in Kauf genommen wurden, um das Geld für ein paar Schlüssel zu sparen.

Im Rahmen der unter Textziffer 6.7.2 dargestellten sicherheitstechnischen Überprüfung der Computersysteme in einem Finanzamt „stolperte" unser Mitarbeiter geradezu über Schwachstellen bei der Verwaltung der Steuerakten. Diese wurden in meist überfüllten zentralen Aktenräumen, in den Büros der Mitarbeiter oder einfach in Kammern gelagert. Die Aktenschränke waren vielfach so alt, daß sie aufgrund ihres desolaten Zustandes nicht mehr abgeschlossen werden konnten. Selbst für die **Personalakten der Bediensteten** waren keine ausreichenden abschließbaren Behältnisse vorhanden. Wegen der angeblich begrenzten finanziellen Mittel wurden in jüngster Zeit in Abstimmung mit der Oberfinanzdirektion statt neuer verschließbarer Schränke offene Regale angeschafft.

Welchen Stellenwert die Wahrung des Steuergeheimnisses in diesem Finanzamt hatte, macht folgendes Beispiel deutlich: Eine über den Flur zu erreichende Kammer war zu einer „Aktenzentrale" umgestaltet worden. Die Tür stand ständig offen, so daß sich jedermann ungehindert Zugang verschaffen konnte. Unser Prüfer hat sich jedenfalls mehrfach unbeobachtet im Raum aufgehalten und hätte ungehindert auf hunderte von Akten aus dem Bereich „gewerbliche Veranlagung" (wesentlicher Inhalt: Bilanzen, Gewinn- und Verlustrechnungen, Betriebsprüfungsberichte usw.) zugreifen können. Dem verantwortlichen Sachgebietsleiter war diese Situation bekannt. Ein regelmäßiges Verschließen der Tür und die Aufbewahrung des Schlüssels an einer zentralen Stelle erschien ihm jedoch nicht zumutbar, da eine größere Anzahl von Mitarbeitern häufig Akten entnehmen und wieder einsortieren müßten. Für die Bereitstellung mehrerer Schlüssel seien **keine finanziellen Mittel** vorhanden.

Diese Aussage ist vor dem Hintergrund zu sehen, daß der Steuerverwaltung für derartige Sachmittel im letzten Haushalt über 500 000 DM zur Verfügung stan-

den. Geld für ein paar Schlüssel sollte da abzuzweigen sein. In der Tat ist dieser Mangel nach unserer **Beanstandung** vom Finanzamt abgestellt worden. Ansonsten hat es sich auf eine recht formale Position zurückgezogen: Die Mitarbeiter seien durch eine Dienstanweisung gehalten, die Akten so zu verwahren, daß es zu Verletzungen des Steuergeheimnisses nicht kommen könne. Es werde künftig verstärkt auf ihre Einhaltung geachtet und somit „den an den Datenschutz zu stellenden Mindestanforderungen genügt". Wir werden uns zu gegebener Zeit durch eine Nachprüfung ein eigenes Bild machen!

Was ist zu tun?
Für Daten, die einem „besonderen" Amtsgeheimnis unterliegen, sind auch „besondere" Sicherheitsmaßnahmen zu treffen. Fahrlässig handelt, wer, anstatt ein wirksames Sicherheitskonzept zu entwickeln, nur versucht, den Mindestanforderungen zu genügen.

4.11 Personalwesen

4.11.1 Modernes Personalmanagement datenschutzgerecht gestalten

Verwaltungsmodernisierung ist das Gebot der Stunde. Mangelnde Bürgernähe und Transparenz, fehlende Effektivität und Flexibilität, aber vor allem zu hohe Kosten sind Anlaß dafür, die Strukturen der Verwaltung grundlegend zu überdenken. Ein Gestaltungselement hierbei ist auch der Datenschutz.

Die für die Verwaltungsmodernisierung maßgeblichen neuen Leitbilder stammen durchgängig aus der Privatwirtschaft. Sie sollen das überkommene Selbstverständnis der preußischen Obrigkeitsverwaltung ablösen. Bei der Übernahme **privatwirtschaftlicher Managementmethoden** kommt es jedoch zwangsläufig zu Konflikten mit rechtlichen Regelungen, die mit dem neuen Verwaltungsinstrumentarium nicht kompatibel sind. Dies gilt auch für das Datenschutzrecht. Das deutsche Datenschutzrecht basiert auf der Trennung von privatem und öffentlichem Bereich. Im öffentlichen Bereich gilt ein strenger Gesetzesvorbehalt mit der Erwartung bereichsspezifischer normenklarer Regelungen; im Privatbereich finden sich häufig dehnbare Generalklauseln. Outsourcing und Privatisierung stoßen deshalb an datenschutzrechtliche Grenzen. Ein Problemfeld sind moderne Personalmanagementmethoden, die sich an den Bestimmungen zum Schutz von Personaldaten messen lassen müssen. Im Berichtszeitraum hatten wir u. a. folgende Modernisierungsprojekte zu begutachten:

- **Potentialanalyse für Führungskräfte**

> ***Potentialanalyse***
>
> *Die Potentialanalyse für Führungskräfte in der Landesverwaltung dient dem Erkennen und der Förderung von Entwicklungsmöglichkeiten bei Bediensteten, die Führungsfunktionen wahrnehmen (sollen). Zu diesem Zweck sollen alle Führungskräfte ein Personalentwicklungsseminar durchlaufen, in dem die Qualität und potentielle Fähigkeiten von höheren Bediensteten erkundet und bewertet werden.*

Unter dem Vorsitz der Staatskanzlei erarbeitete eine ressortübergreifende Projektgruppe Vorschläge zur Verbesserung der Personalentwicklung für Führungskräfte in der Landesverwaltung. Ziel dieser Reformmaßnahmen ist das Erkennen von **personellem Potential**, die Qualifizierung von Nachwuchskräften und das Aufzeigen und Fördern individueller Entwicklungsmöglichkeiten. Zentraler Bestandteil dieser Personalentwicklung ist die auf freiwilliger Basis erfolgende Potentialanalyse, die der Ermittlung individueller Fähigkeitsprofile dient. Hierfür werden verschiedene Erkenntnisquellen herangezogen und – als zentrales Element – Personalentwicklungsseminare durchgeführt. An der Durchführung beteiligt sind externe Berater/innen und Mitarbeiter/innen der Personalverwaltungen verschiedener Ressorts. Das Ergebnis des abschließenden Potentialgesprächs soll Eingang in die Personalakte finden und künftig Grundlage bei der Personalauswahl und Stellenbesetzung sein.

Gegen die Zielsetzung der Projektgruppe ist nichts einzuwenden. Wir haben aber darauf hingewiesen, daß bezüglich aller Maßnahmen des Personalentwicklungskonzeptes, bei denen personenbezogene Daten verarbeitet werden, die Beachtung des Datenschutzrechts selbstverständlich sein muß. Das **Personalaktenrecht**, das immer anwendbar ist, wenn das Grundverhältnis der Bediensteten zum Dienstherrn betroffen ist, enthält strenge Abschottungs-, Zweckbindungs- und Übermittlungsregelungen, die auch bei der ressortübergreifenden Organisation beachtet werden müssen.

Bei der Konzeption der **Potentialanalyse** stellte sich die Frage, inwieweit hierbei **externe Berater** und **ressortfremde Mitarbeiter** der Landesverwaltung einbezogen werden dürfen. Wir stellten klar, daß diese nicht befugt sind, in Personalakten Einblick zu nehmen. Soweit die Bewertungen als Bestandteil der Potentialanalyse künftig in Personenauswahlentscheidungen einfließen sollen, so muß dies ausdrücklich gesetzlich geregelt werden.

Inwieweit diese rechtlichen Vorgaben auch für ressortfremde Mitarbeiter/innen des Landes gelten, wird ebenfalls noch abschließend zu klären sein. Von der Rechtmäßigkeit dieses Verfahrens hängt es schließlich ab, ob das Ergebnis des abschließenden Potentialgesprächs in die Personalakte aufgenommen werden kann. Unsere rechtliche Bewertung wurde bei der Beschlußfassung über das Personalentwicklungskonzept bereits teilweise berücksichtigt. Für die verbleibenden Fragen ist abzuwarten, ob sich Lösungen finden lassen, die allen beteiligten Interessen gerecht werden.

- **Kosten-Leistungs-Rechnung**

Ziel der KLR ist es, die Kosten der von der Verwaltung erbrachten Leistungen sowie die hierbei erwirtschafteten Erträge festzustellen. Damit soll **Kostentransparenz** für alle Beteiligten, aber auch mehr **Kostenverantwortung** der Bediensteten, erreicht werden. Zumindest mittelfristig soll mit Hilfe der KLR auch die Leistungsverrechnung mit anderen Stellen der öffentlichen Verwaltung und von Dienstleistungen für die Bürgerinnen und Bürger erfolgen.

> ***Kosten-Leistungs-Rechnung (KLR)***
>
> *Mit der KLR werden die kostenrelevanten Positionen der Verwaltung elektronisch so erfaßt, daß sie einzelnen Leistungen (z. B. Ausstellung eines Personalausweises, Erlaß einer Baugenehmigung) zugeordnet werden können. Dadurch wird erkennbar, welchen tatsächlichen Aufwand die Erbringung bestimmter Leistungen verursacht hat. Eingang finden auch der Arbeitsaufwand und die dadurch verursachten Personalkosten.*

Da **Personalkosten** in diesem Zusammenhang ein wesentlicher Aspekt sind, geraten die Besoldungs- und Leistungsdaten der Bediensteten ins Blickfeld der KLR. Als Handreichung für die Verwaltung haben wir deshalb aus den gesetzlichen Regelungen Kriterien abgeleitet, mit denen ein Konflikt zwischen diesen neuen Analysemethoden und dem Personaldatenschutzrecht vermieden wird:

- Vor der Einführung der KLR, bei der personenbezogene Daten verarbeitet werden, sind die damit verfolgten Zielsetzungen (Zwecke) eindeutig festzulegen (Transparenz für Stellenleitung, Budgetierung, Leistungsverrechnung).
- Der Personalrat ist zu beteiligen. Dienstvereinbarungen können die näheren Modalitäten der KLR regeln.
- Automatisierte Systeme im Rahmen von KLR sind vor ihrem Wirkbetrieb zu dokumentieren, zu testen und freizugeben. Es muß ein Sicherheitskonzept vorliegen.
- Daten, die im Rahmen von KLR verarbeitet werden sollen, sind, wenn möglich, bei den betroffenen Bediensteten zu erheben.
- Eine Nutzung von Personalaktendaten in personenbeziehbarer Form für den Zweck der Leistungsverrechnung ist unzulässig. Entsprechende Daten sind zuvor zu anonymisieren.
- Die Verarbeitung von Urlaubs- und Krankheitsdaten von Bediensteten in personenbeziehbarer Form ist unzulässig.
- Die Nutzung von KLR-Daten für Verhaltens- und Leistungskontrollen der Bediensteten ist unzulässig.
- Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt (d. h. wenn kein Personenbezug mehr erforderlich ist) zu löschen oder zu anonymisieren. Ist dies nicht möglich, so hat eine Teilanonymisierung zu erfolgen.
- Eine Anonymisierung von Daten kann durch folgende Maßnahmen erfolgen:

Zusammenfassung von Personalstellen zu größeren organisatorischen Einheiten, Aggregieren von Datensätzen, Löschen von Referenzlisten, Standardisierung arbeitsplatzbezogener Kosten- und Leistungsstellen.

- Die KLR betreibende Organisationseinheit ist von der Personalabteilung sowie von den sonstigen sachbearbeitenden Abteilungen organisatorisch, personell und räumlich abzuschotten.

Bei den uns bisher bekannt gewordenen Projekten in diesem Bereich konnten wir feststellen, daß diese Kriterien beachtet werden.

- **Unzulässiges Outsourcing**

Das Ministerium für Umwelt, Natur und Forsten plante die Zusammenlegung der in unterschiedlichen Behörden untergebrachten Laboreinrichtungen. In die Prüfung des dadurch bestehenden Einsparpotentials wurde eine **private Firma als Gutachter** mit einbezogen. Diese sollte mit Hilfe der personenbezogenen Daten über Besoldung, sonstige Personalkosten sowie Alter und Dienstverhältnis der einzelnen Mitarbeiter der verschiedenen Labore eine Analyse vornehmen. Gegen die Nutzung von Personalaktendaten meldete der Personalrat berechtigte Bedenken an. Das Ministerium ging zunächst davon aus, daß die Gutachtenerstellung durch die private Firma als Auftragsdatenverarbeitung zulässig sei. Tatsächlich handelte es sich aber nicht um eine reine Hilfstätigkeit bei der Datenverarbeitung, sondern um eine eigenverantwortliche Datennutzung. Demgemäß war die Weitergabe von Personalunterlagen an die Firma rechtlich eine Datenübermittlung, die unter den gegebenen Umständen nur mit Einwilligung der Betroffenen zulässig gewesen wäre. Diese Argumente überzeugten das Ministerium. Der private Gutachter wurde aufgefordert, die dort schon vorhandenen Personalerhebungsbögen zurückzusenden und die entsprechenden Aufzeichnungen zu vernichten. Die für den Gutachtenauftrag benötigten Auswertungen werden nun vom Ministerium selbst vorgenommen und dann in anonymisierter Form an die Gutachter übersandt.



4.11.2 Der Blick des behördlichen Datenschutzbeauftragten in die Personalakte

Behördliche Datenschutzbeauftragte dürfen im Rahmen ihrer Kontrolltätigkeit Einblick in Personalakten nehmen, wenn sie hierzu den Auftrag von der Behördenleitung erhalten haben.

Anders als in anderen Ländern (z. B. Berlin, Hessen, Niedersachsen) gibt es zum **behördlichen Datenschutzbeauftragten** im Landesdatenschutzgesetz Schleswig-Holstein (LDSG) noch keine Regelung. Dies wird sich wahrscheinlich erst mit der Novellierung des LDSG aus Anlaß der Anpassung an die Europäische Datenschutzrichtlinie (EG-DSRL) ändern, da hierin die „unabhängige Überwachung" durch einen internen Datenschutzbeauftragten vorgeschrieben ist.

Die Bestellung eines behördlichen Datenschutzbeauftragten halten wir jedoch schon heute für dringend geboten. Wie die Funktion wahrgenommen wird, bestimmt allerdings im Rahmen seiner **Organisationshoheit die Leiterin bzw. der Leiter** der betreffenden öffentlichen Stelle. Das Landesbeamtengesetz sieht vor, daß Zugang zu Personalakten nur erhalten darf, wer „im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt" ist. Eine solche Beauftragung kann sich auch auf die Kontrolle des Datenschutzes in Personalangelegenheiten beziehen. Die Nutzung von Daten zu Zwecken der Datenschutzkontrolle bedeutet dann keine unzulässige Zweckänderung. Die Beauftragung des behördlichen Datenschutzbeauftragten mit der Kontrolle von Personalakten ist auch sinnvoll, weil die Eigenkontrolle durch die Mitarbeiter der Personalverwaltung nicht ausreichend ist.

Was ist zu tun?
Behördliche Datenschutzbeauftragte dürfen im Auftrag der Behördenleitung auch die Korrektheit der Personalaktenverwaltung überprüfen.

4.11.3 Verfahren zur Unterrichtung unterlegener Bewerber

Die notwendige Unterrichtung eines unterlegenen Bewerbers über die entscheidenden Wertungsfaktoren kann schon vor einer abschließenden schriftlichen Auswahlentscheidung des Dienstherrn erfolgen.

Im Rahmen eines Bewerberausleseverfahrens war einem unterlegenen Bewerber Einsicht in die aus diesem Anlaß gefertigte **Beurteilung** des **Konkurrenten** gewährt worden. Dieser machte hiergegen datenschutzrechtliche Bedenken geltend, insbesondere mit der Begründung, die Unterrichtung sei unzulässigerweise bereits vor der schriftlichen Entscheidung erfolgt.

Das **Schleswig-Holsteinische Oberverwaltungsgericht** hat schon entschieden, daß ein Mitbewerber verlangen kann, vor der Beförderung eines Kollegen über Auswahl und Verfahren informiert zu werden. Zur Gewährleistung eines effektiven Rechtsschutzes sei es erforderlich, dem unterlegenen Bewerber auch die entscheidenden Wertungsfaktoren zugunsten des obsiegenden Konkurrenten mitzuteilen. Nur in Kenntnis dieser Daten könne er effektiv prüfen, ob sein Anspruch auf rechtsfehlerfreie Bescheidung seiner Bewerbung unter Beachtung des Leistungsprinzips verletzt wurde.

Um ihren Zweck zu erfüllen, muß die Unterrichtung nach unserer Auffassung eine angemessene Zeit vor der Entscheidung erfolgen, da diese nach Vollzug nicht mehr rückgängig gemacht werden kann. Die Ablehnung einer Bewerbung ist ein Verwaltungsakt, da sich diese unmittelbar auf die statusrechtliche Stellung des Betroffenen auswirkt. Nach dem Landesverwaltungsgesetz sind in die Begründung des Verwaltungsaktes die wesentlichen tatsächlichen und rechtlichen Gründe aufzunehmen, die die Behörde zu ihrer Entscheidung bewogen haben. Bei einer **Eignungsprüfung** genügt zunächst eine mündliche Begründung. Auf Antrag ist

jedoch diese schriftlich zu erteilen. Dieser Antrag kann nur innerhalb einer Frist von zwei Wochen nach Bekanntgabe des Verwaltungsaktes gestellt werden. Die Begründung einer Personalausleseentscheidung muß also zumindest mit der Bescheiderteilung in mündlicher Form erfolgen. Der mündlichen Auskunftserteilung steht eine Bereitstellung von Unterlagen zur Einsichtnahme gleich. Wird einer Ausleseentscheidung eine aus diesem Anlaß gefertigte Beurteilung als Ganzes zugrunde gelegt, kann sich der Informationsanspruch auch auf den gesamten Inhalt der Beurteilung erstrecken.

In dem geprüften Fall bestanden auch keine Bedenken dagegen, daß die Unterrichtung über die gefertigte Anlaßbeurteilung bereits vor der schriftlichen Entscheidung erfolgt war, da der Dienstherr sich im Zeitpunkt der Unterrichtung bereits dahin gehend festgelegt hatte, die Anlaßbeurteilung als Ganzes für die zu treffende Auswahlentscheidung zugrunde zu legen. Die **Unterrichtung der Mitkonkurrenten** in Bewerberausleseverfahren steht im Einklang mit den Regelungen des Landesbeamtengesetzes zur Verarbeitung von Personalaktendaten. Danach ist sie u. a. auch ohne Einwilligung des Beamten zulässig, wenn der Schutz berechtigter höherrangiger Interessen der oder des Dritten die Auskunftserteilung zwingend erfordert. Bei Konkurrentenstreitigkeiten bestehen die berechtigten höherrangigen Interessen des Mitkonkurrenten gerade in der Gewährleistung eines effektiven Rechtsschutzes.



Was ist zu tun?
Zur Gewährleistung eines effektiven Rechtsschutzes der Betroffenen ist es zulässig, Mitbewerber in Personalausleseverfahren rechtzeitig über die entscheidenden Wertungsfaktoren zu unterrichten.

4.11.4 Versendung von amtsärztlichen Gutachten auf dem Dienstweg

Amtsärztliche Gutachten gehören zu den besonders sensiblen Unterlagen in der Personalakte. Ihre Versendung „auf dem Dienstweg" führt zwangsläufig zu einer Verletzung des Personalaktengeheimnisses.

Nach längerem Leidensweg sollte ein Lehrer wegen Dienstunfähigkeit in den Ruhestand versetzt werden. Auf Anforderung erhielt er vom Bildungsministerium sein amtsärztliches Gutachten **auf dem Dienstweg**, d. h. nach Kenntnisnahme durch den Schulleiter, übersandt. Zur Geschäftserleichterung war gleich noch eine Berechnung seiner ruhegehaltsfähigen Dienstzeit beigefügt. Auf unsere Nachfrage berief sich das Bildungsministerium auf seinen Erlaß, wonach Dienstpost in Personalangelegenheiten als solche deutlich zu kennzeichnen und – für jeweils eine Schule gesammelt – in verschlossenen Umschlägen mit der Aufschrift „Schulleiter o. V. i. A." zu versenden ist.

In dem hier zu beurteilenden Fall lag die Zuständigkeit für die dienstrechtliche Bewertung der mit dem amtsärztlichen Gutachten erhobenen Gesundheitsdaten ausschließlich beim Bildungsministerium. Auch für die Berechnung der ruhege-

haltsfähigen Dienstzeit bestand keine Zuständigkeit des Schulleiters. Seine Unterrichtung war nicht erforderlich. Der Erlaß über die Versendung von Personalunterlagen kann sich nur auf solche Unterlagen beziehen, die für die Aufgabenerfüllung des Schulleiters tatsächlich benötigt werden. Andere Unterlagen sind den Betroffenen im **verschlossenen Umschlag** direkt zuzuleiten.



Die unzulässige Offenbarung von Personalaktendaten haben wir gegenüber dem Bildungsministerium beanstandet. Außerdem waren die beim Schulleiter unzulässigerweise gespeicherten Unterlagen – dieser hatte sich natürlich entsprechende Kopien gefertigt – zu löschen.

Was ist zu tun?
Fachvorgesetzte dürften Personalaktendaten ihrer Mitarbeiter nur zur Kenntnis erhalten, soweit es zu ihrer Aufgabenerfüllung erforderlich ist. Andere Unterlagen müssen von der Personalverwaltung im verschlossenen Umschlag direkt an die Betroffenen versandt werden.

4.12 Angekündigte Unangekündigte Kontrollen (AUK)

Die Ergebnisse der Angekündigten Unangekündigten Kontrollen zeigen, daß in den Verwaltungen zwar überwiegend sorgsam mit personenbezogenen Daten umgegangen wird. Gleichwohl gab es aber fast überall Mängel zu beanstanden. In einzelnen Fällen waren haarsträubende Fehler festzustellen.

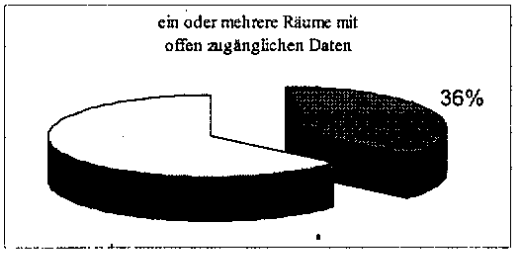
Auch in diesem Berichtsjahr haben wir unser 1996 entwickeltes Konzept der Angekündigten Unangekündigten Kontrollen (AUK) fortgesetzt. Bei diesen Kontrollen wird in erster Linie die **„äußere" Datensicherheit** und der **sorgfältige Umgang mit personenbezogenen Daten** in öffentlichen Stellen geprüft. Insbesondere geht es darum, ob die einzelnen Behörden die ihnen anvertrauten personenbezogenen Daten wirkungsvoll gegen die Einsichtnahme Unbefugter schützen (vgl. 19. TB, Tz. 1.1). Am Jahresanfang hatten wir 50 Behörden angeschrieben und ihnen mitgeteilt, daß sie mit einer unangemeldeten Kontrolle rechnen müßten. Per Los wurden dann neun Stellen für einen Kontrollbesuch ermittelt.

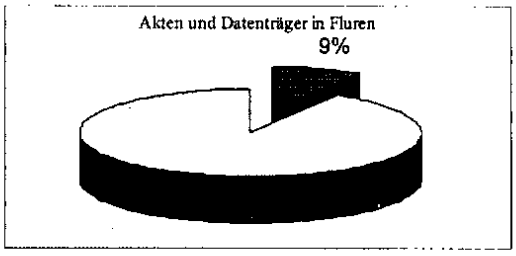
Bei diesen Kontrollen hat sich erneut gezeigt, daß diese Vorgehensweise unsere sonstigen Prüfungen sinnvoll ergänzt. Auch wenn sich anhand der festgestellten Mängel im Vergleich zum Vorjahr generell eine **Verbesserung der Datensicherheit** feststellen läßt, mußten wir wiederum zahlreiche einzelne Beanstandungen aussprechen. Einige Verwaltungen vertrauen offensichtlich noch immer recht sorglos darauf, daß niemand ein offen zugängliches und unbesetztes Büro betritt und dort neugierig Einblick in personenbezogene Unterlagen oder Dateien nimmt. Im EDV-Bereich fehlten häufig die vorgeschriebenen technischen und organisatorischen Maßnahmen und entsprechende Dienstanweisungen. Die Mitarbeiterinnen und Mitarbeiter waren im Hinblick auf die Sicherung ihrer PC gegen unbefugten Zugang häufig nicht ausreichend geschult.

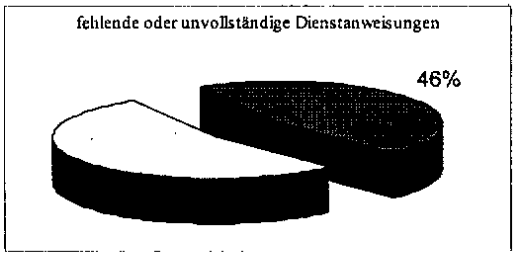
Besondere „**Highlights**“ unserer Kontrollen waren in diesem Jahr:

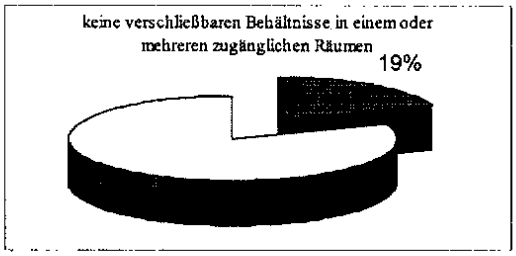
- In einer Behörde fanden wir in einem offenen Raum einen eingeschalteten und ungeschützten PC vor, auf dem sich das Liegenschaftsverzeichnis der Stadt befand. Die darin enthaltenen personenbezogenen Daten hätten ohne weiteres manipuliert werden können, weil der Zugang zur Betriebssystemebene nicht gesichert war. Erschwerend kam hinzu, daß sich die Prüfer in dem Raum zunächst unbehelligt aufhalten konnten. Zwei Mitarbeiter der Verwaltung, die den Raum zwischendurch betraten, wunderten sich nicht über die Anwesenheit behördenfremder Personen und entfernten sich höflich, nachdem ihnen von den Prüfern erklärt worden war, daß „die Arbeiten an dem PC noch einige Zeit in Anspruch nehmen würden“.
- Das Sozialamt einer Amtsverwaltung hatte offensichtlich gerade den „Tag der offenen Türen“ ausgerufen. Unsere Prüfer konnten die unbesetzten Büros betreten, sich Akteninhalte ansehen und über den eingeschalteten, nicht gesicherten PC Einblick in die dort enthaltenen Daten der Wohngeldempfänger nehmen. Es wäre auch ohne weiteres möglich gewesen, Veränderungen am Datenbestand vorzunehmen. Erst geraume Zeit später kehrte die Mitarbeiterin zurück und fragte empört, wieso wir auf die Idee kämen, ihr – weit offenstehendes – Büro „einfach so“ zu betreten.
- In einer Amtsverwaltung war es den Prüfern möglich, in den Serverraum zu gelangen, weil dessen Tür nur angelehnt war. Der Server selbst war nicht durch ein Paßwort geschützt. Dadurch wäre es möglich gewesen, auf alle dort zentral gespeicherten Daten zuzugreifen, um diese beispielsweise zu löschen oder zu verändern.
- Bei einer Gemeindeverwaltung mußten wir im unbesetzten Büro des EDV-Administrators feststellen, daß man sich dort trotz offener Tür zum Nebenzimmer ungestört umsehen konnte. Dabei stellte sich heraus, daß der Bildschirm des laufenden PC nur dunkel geschaltet und nicht mit einem Paßwort gesichert war. Von hier aus wäre es möglich gewesen, Zugriff auf sämtliche Bereiche des Server-Netzwerkes der Behörde zu nehmen. Ausgerechnet der PC des Administrators verfügte über keinerlei Sicherungsmöglichkeiten des Bildschirms.

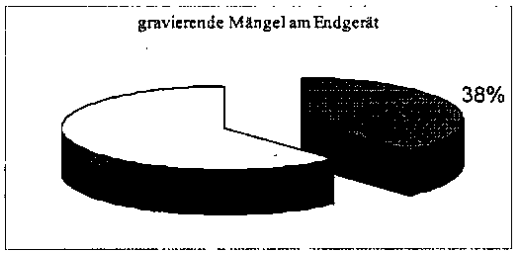
Die nachfolgenden Diagramme vermitteln einen Gesamtüberblick über das Ergebnis der von uns seit 1996 durchgeführten Kontrollen bei insgesamt 21 Behörden:

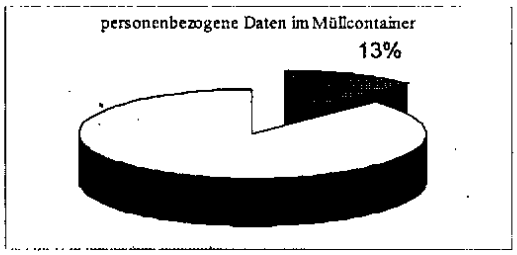


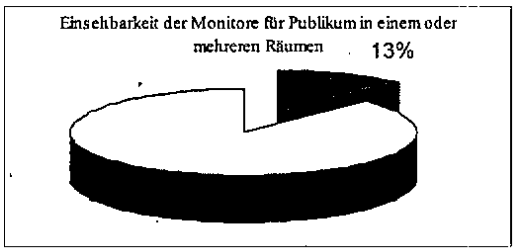


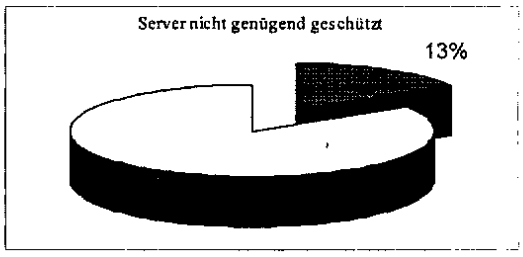


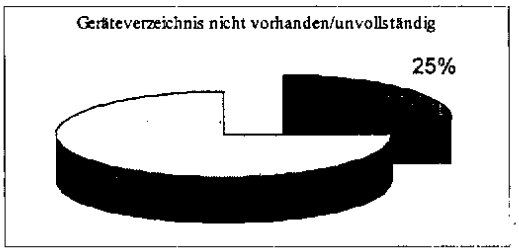












5. Datenschutz bei Gerichten

5.1 Elektronisches Grundbuch

Nach den Staatsanwaltschaften und den Gerichten sollen jetzt auch die Grundbuchämter in Schleswig-Holstein auf elektronische Datenspeicherung umstellen. Im Hinblick auf die enorme wirtschaftliche Bedeutung der in Grundbüchern vorgehaltenen Daten sind hier an die Datensicherheit höchste Ansprüche zu stellen.

Die rechtlichen Grundlagen für die Führung elektronischer Grundbücher hat der Gesetzgeber im Jahr 1993 durch das **Registerverfahrenbeschleunigungsgesetz** geschaffen. In einigen Bundesländern werden derartige Verfahren schon eingesetzt. In Schleswig-Holstein ist eine Initiative, die im Frühjahr 1997 gemeinsam mit dem Land Mecklenburg-Vorpommern gestartet wurde, soweit gediehen, daß noch im Jahre 1999 das erste elektronische Grundbuch (EGB) in Betrieb genommen werden soll.

Die beteiligten Länder gehen davon aus, daß ein EGB „deutlich erhöhte Anforderungen an die Verfügbarkeit, die **Datensicherheit**, den Datenschutz und die nachhaltige Wartbarkeit" stellt als die bisherige papierbasierte Verfahrensweise. Tatsächlich kommt der Datensicherheit im Hinblick auf die enormen Werte, die jeder einzelne Grundbucheintrag verkörpern kann, eine entscheidende Bedeutung zu.

Zudem wirft die Frage der "**Zukunftsfähigkeit**" des EGB erhebliche Probleme auf, weil sich der Zeithorizont bei der Führung des Grundbuchs in einer anderen Größenordnung darstellt als die Halbwertzeit heutiger Softwareprodukte. Beim EGB geht es nicht um Jahre oder Jahrzehnte; vielmehr muß sichergestellt sein, daß die Speicherungen hundert Jahre und länger nachvollziehbar bleiben. Für das Speichermedium Papier wurde diese Anforderung über die Qualität des Materials gelöst. Wie eine derartig lange Nachvollziehbarkeit von elektronisch gespeicherten Daten technisch gewährleistet werden kann, ist zumindest zum Projektstart noch offen.

Die Verantwortlichen in den Justizministerien haben sich dafür entschieden, nicht auf die bereits existierende Software zweier großer Anbieter, die in anderen Bundesländern zum Einsatz kommt, zurückzugreifen. Statt dessen soll durch ein privates Softwarehaus eine für die beiden Länder **maßgeschneiderte Lösung** erstellt werden. Die Projektverantwortlichen versprechen sich durch ihre Eigenentwicklung eine größere Unabhängigkeit von marktbeherrschenden Anbietern und den von ihnen zu erwartenden schnellen Generationenfolgen der Software.

- **Zukunftsplanung: Online-Auskunft über das Internet**

Für das Jahr 1999 ist die Realisierung der ersten Ausbaustufe des Projekts angestrebt, die die softwaregestützte Abwicklung der Eintragungen und die Datenbankverwaltung umfaßt. In einer zweiten Ausbaustufe soll dann auch die **Grundbuchauskunft** in einem automatisierten Verfahren möglich werden. Jedermann steht bei Vorliegen eines berechtigten Interesses das Recht auf Einsicht in das Grundbuch zu. Bei Notaren und Behörden entfällt sogar die Prüfung des berechtigten Interesses. Diese Personen und Institutionen sollen künftig über das Internet Zugriff auf die Daten erhalten. Wegen des unsicheren Übertragungsmediums „Internet" werden hier die höchstmöglichen Sicherheitsstandards zur Anwendung kommen müssen. Dazu wird auch gehören, daß die berechtigten Abfrager sich mittels einer digitalen Signatur authentisieren (vgl. 19. TB, Tz. 7.7; 20. TB, Tz. 7.2).

In der Vergangenheit mußten wir das Justizministerium davon überzeugen, daß die Grundbuchauskünfte aus dem konventionell geführten Grundbuch mit guten Gründen einzeln **protokolliert** werden (vgl. 15. TB, Tz. 4.3.8; 16. TB, Tz. 9; 17. TB, Tz. 9.1). Auf diesen Nachweis der Berechtigung kann auch bei elektronischen Auskünften nicht verzichtet werden. Eine Protokollierung nur bestimmter Abrufe wäre nicht ausreichend.

- **Wie unterschreibt der Grundbuchbeamte elektronisch?**

Im herkömmlichen Grundbuch leisten die für die Führung des Grundbuchs zuständige Person und der Urkundsbeamte der Geschäftsstelle ihre **Unterschrift** unter jeden Eintrag und bestätigen so mit ihren Namen dessen Richtigkeit. Im Projekt EGB muß man sich mit der Frage beschäftigen, wie die Unterschriften und ihre Sicherungs- und Bestätigungsfunktion in **elektronischer Form** abgebildet werden können. Die Grundbuchverordnung fordert, daß der Urkundsbeamte der Geschäftsstelle der Eintragung seinen Namen hinzusetzt und „beides elektronisch unterschreibt". Diese elektronische Unterschrift soll in einem „allgemein als sicher anerkannten automatisierten kryptographischen Verfahren text- und unterzeichnerabhängig hergestellt werden".

> ***Im Wortlaut: § 75 GBV***
>
> *Bei dem maschinell geführten Grundbuch soll eine Eintragung nur möglich sein, wenn die für die Führung des Grundbuchs zuständige Person oder, in den Fällen des § 74 Abs. 1 Satz 3, der Urkundsbeamte der Geschäftsstelle der Eintragung ihren oder seinen Nachnamen hinzusetzt und beides elektronisch unterschreibt. Die elektronische Unterschrift soll in einem allgemein als sicher anerkannten automatisierten kryptographischen Verfahren textabhängig und unterzeichnerabhängig hergestellt werden. Die unterschriebene Eintragung und die elektronische Unterschrift werden Bestandteil des maschinell geführten Grundbuchs. Die elektronische Unterschrift soll durch die zuständige Stelle überprüft werden können.*

Das bedeutet, daß eine Eintragung auch Jahre nach der Speicherung der tatsächlich handelnden Person zugeordnet werden können muß. Dies kann nur in Form

einer „**digitalen Signatur**" erfolgen (vgl. 19. TB, Tz. 7.7; 20. TB, Tz. 7.2). Eine solche Signatur sollte sich an den Sicherheitsstandards des Signaturgesetzes orientieren. Jeder zur Eintragung ins Grundbuch berechtigte Mitarbeiter müßte eine **Chipkarte** erhalten, die seinen persönlichen Schlüssel enthält. Im Anschluß an die eigentliche Eintragung würde mit dem persönlichen Schlüssel eine Signatur erzeugt, deren Nachahmung oder Fälschung technisch ausgeschlossen ist. Auf diese Weise würde das bisher in Papierform praktizierte Verfahren am besten in elektronischer Form abgebildet. Wie bei der Unterschrift auf Papier würde durch eine eindeutige, bewußt vorgenommene Handlung die Echtheit der Eintragung bestätigt Der Eintragende trüge die Verantwortung dafür, daß die ausschließlich ihm gewährten Rechte nicht mißbraucht werden. Dazu gehört, daß auf die sichere Verwahrung der Chipkarte geachtet und jede Unregelmäßigkeit gemeldet werden muß.

Noch ist nicht klar, ob der Justizminister dieses Verfahren realisieren wird. Es scheint so, daß die Datensicherheit möglicherweise hinter das Ziel der schnellen Realisierung und der Kostenminimierung zurücktreten soll. Zur Zeit wird ein Verfahren entwickelt, bei dem den zur Eintragung berechtigten Mitarbeitern keine persönlichen Schlüssel zugeordnet werden. Statt dessen soll es lediglich einen „**Schlüssel des Prozesses**" geben, der vom Rechner automatisch vergeben wird, sich jedoch nicht im Hinblick auf die einzelnen Mitarbeiter unterscheidet. Wird auf den Einsatz **personalisierter Schlüssel** verzichtet, so ist zu befürchten, daß die Sicherheit des Verfahrens insgesamt absinkt. Im Vergleich zum herkömmlichen Grundbuch hat beim EGB ein erweiterter Personenkreis Zugriff auf die Grundbuchdaten: die mit der Systemadministration befaßten Personen und zum Teil die Personen, die Zugriff auf die Leitungen und die Knotenrechner haben. Aus unserer Sicht kann ein personalisierter Schlüssel am besten ausschließen, daß von Personen mit Administrationsrechten Manipulationen vorgenommen werden, die nachträglich nicht mehr bemerkbar wären. Der aus unserer Sicht erforderlichen Methode wird entgegengehalten, daß sie nur zu realisieren sei, wenn ein vertrauenswürdiger Dritter (auch: Trustcenter oder Zertifizierungsstelle) existiere, der die Chipkarten ausgebe und ihre Zuordnung zu dem jeweiligen Empfänger garantiere.

- **Es fehlen öffentliche Trustcenter**

Dieser Einwand legt ein grundsätzliches Defizit beim Einstieg der Verwaltung in die digitale Vorgangsbearbeitung und Kommunikation offen: Bestimmte Staatsaufgaben sind für die Gesellschaft so wichtig, daß sie nur von staatlichen Stellen und durch öffentlich Bedienstete und trotz aller Privatisierungstendenzen nicht privat erbracht werden dürfen. Dazu gehört die Führung eines Grundbuches als grundlegender Nachweis der Eigentumsverhältnisse an Grundstücken.

Ist dabei systembedingt der Einsatz einer **vertrauenswürdigen dritten Stelle** nötig, so ist es Teil der staatlichen Aufgabe, eine solche Instanz zur Verfügung zu stellen. Zwar müssen auch die privaten Zertifizierungsstellen nach dem Signaturgesetz hohen technischen und organisatorischen Ansprüchen genügen. **Staatliche Trustcenter** wären jedoch für die Verwaltungsanwendungen allein schon deswe-

gen verläßlicher, weil sie sich nicht am Markt behaupten müßten und nicht wegen wirtschaftlicher Probleme eines Tages den Betrieb einstellen könnten.

Auch bei anderen Anwendungen der elektronischen Kommunikation zwischen Behörden wird es künftig nicht mehr ohne den Einsatz von digitalen Signaturen gehen. Aus unserer Sicht ist es daher dringend geboten, daß ein oder mehrere **staatliche Trustcenter** für die Verwaltungsanwendungen aufgebaut werden. Verfügte das Justizministerium über ein solches Trustcenter, so wäre der Einsatz personalisierter Schlüssel im Verfahren EGB kein Problem. Bedenklich erscheint uns, daß man bisher noch nicht einmal ermittelt hat, wie groß der Aufwand für ein **grundbuchspezifisches internes Trustcenter** sein wird. Er dürfte geringer sein als gemeinhin angenommen. Wird auf die Vergabe personalisierter Schlüssel verzichtet, so muß der dadurch eintretende Verlust an Manipulationssicherheit durch zusätzliche technische und organisatorische Maßnahmen aufgefangen werden.

Was ist zu tun?
Das Justizministerium sollte beim Verfahren EGB keine Abstriche bei der Datensicherheit machen und die elektronische Unterschrift als digitale Signatur ausgestalten.

5.2 Nichtöffentliche Verhandlungen vor Finanzgerichten – Theorie und Praxis

Der Anspruch auf öffentliche Gerichtsverhandlungen soll den Bürgern einen fairen Prozeß sichern. Manchmal verkehrt sich dieses Recht aber ins Gegenteil. Deshalb ist es wichtig zu wissen, wann man nichtöffentliche Sitzungen der Gerichte beantragen kann.

„Ja, warum hat mir das denn niemand gesagt?", fragte eine Petentin erbost, als sie unsere Antwort auf die Frage erhielt, warum eine sie betreffende Sitzung des Finanzgerichts öffentlich gewesen sei. Ihre Erregung war begründet. Es war folgendes geschehen: Durch Fristversäumnisse waren Steuerbescheide rechtskräftig geworden, aufgrund derer sie nach ihrer Auffassung zu hohe Steuern zu zahlen hatte. Das Finanzamt hatte die Einsprüche abgelehnt. Als letzte Chance blieb ihr deshalb nur die Klage vor dem Finanzgericht und die Hoffnung auf einen milden Richter. Groß war jedoch ihr Erstaunen, als sie im Gerichtssaal ein Auditorium von 50 Personen vorfand, das diese öffentliche Verhandlung offensichtlich zu Ausbildungszwecken miterleben wollte. Sollte sie vor diesem Kreis wildfremder Menschen nun die Familienstreitigkeiten verbreiten, die dazu geführt hatten, daß vom Ehepartner keine Steuererklärungen abgegeben worden waren? Wegen dieser Versäumnisse waren nämlich durch das Finanzamt (mit einem Sicherheitszuschlag hinsichtlich der Einkommenshöhe versehene) Schätzungen erfolgt. Wie sollte sie aber anders das Gericht davon überzeugen, daß in diesem speziellen Fall ein eventueller Ermessensspielraum weit auszulegen sei? Am Ende der Verhandlung hatte sie das Gefühl, an der Darlegung ihrer „tragenden" Argumente gehindert gewesen zu sein. Das Gericht wies ihre Klage ab.

Zu der unbefriedigenden Situation hätte es gar nicht kommen müssen. Die bereits 1965 in Kraft getretene Finanzgerichtsordnung enthält eine „Spezialregelung", nach der ein Ausschluß der Öffentlichkeit zu erfolgen hat, „wenn ein Beteiligter, der nicht Finanzbehörde ist, es beantragt." Die Antragsmöglichkeit erklärt sich aus dem Steuergeheimnis. Der Antrag bedarf nicht einmal einer Begründung. Eine Ablehnung wäre nicht zulässig. Die eingangs zitierte Frage der Petentin ist also nur zu verständlich.

Was ist zu tun?

Die Verhandlungsführung der Gerichte und die Beratungsleistungen von Steuerberatern und Anwälten unterliegen nicht der Kontrolle des Landesbeauftragten für den Datenschutz. Deshalb kann er nur an die Beteiligten appellieren, die Betroffenen über die Möglichkeiten aufzuklären, die der Gesetzgeber zur Wahrung des informationellen Selbstbestimmungsrechts geschaffen hat, übrigens lange bevor es Datenschutzgesetze gab.

6. Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung

6.1 Das „Jahr-2000-Problem" – und was das mit dem Datenschutz zu tun hat

Die Schwierigkeiten bei der Anpassung der Computersysteme zeigen, daß die Ursachen vieler Sicherheitsrisiken systematischer Natur sind. Werden die Systeme nicht transparenter, werden wir bald ein permanentes „Jahr-2000-Problem" haben.

Das Kernproblem der Computer mit Beginn des 1. Januar im Jahr 2000 besteht darin, daß ihre Programmierer in den letzten dreißig Jahren Speicherplatz sparen wollten, indem sie bei Jahreszahlen die ersten beiden Stellen wegließen. Damit können die Rechner das Jahr 2000 nicht von dem Jahr 1900 unterscheiden. Sie wissen nicht, ob jemand, für den als Geburtsdatum der 28.02.00 gespeichert ist, ein Greis oder ein Säugling ist, da für beide als Jahr nur „00" abgelegt wurde. Bei allen Rechenoperationen, die sich auf ein aktuelles Datum beziehen (Fristabläufe, Zinsberechnungen usw.), kommen die Rechner also „ins Schleudern", wenn sie in der verbleibenden Zeit bis zum 31.12.1999 nicht auf vierstellige Jahreszahlen umgestellt werden.

Nach unseren bisherigen Erkenntnissen ergeben sich aus dem Jahr-2000-Problem nur in wenigen Fällen unmittelbare **datenschutzrechtliche Konsequenzen**. Es ist allerdings nicht auszuschließen, daß nach dem Jahrtausendwechsel

- Zugangs- und Kontrollsysteme nicht mehr bestimmungsgemäß arbeiten,
- Paßwortwechsel nicht mehr angestoßen werden,
- Löschungsfristen nicht eingehalten werden oder
- Informationssysteme falsche Auskünfte geben, weil die Programme, die sie aktualisieren sollten, nicht funktionieren.

Das Jahr-2000-Problem zeigt darüber hinaus **grundsätzliche Strukturmängel** auf, die von erheblicher datenschutzrechtlicher Bedeutung sind. Seit Jahren warnen wir vor den Folgen der weitverbreiteten Nachlässigkeiten bei der Dokumentation automatisierter Verfahren. Bei den meisten Behörden stießen wir bisher allerdings auf taube Ohren. Selbst die einschlägigen Vorschriften der 1994 in Kraft getretenen Datenschutzverordnung haben nicht dazu geführt, daß für EDV-Programme genau so exakte Bauzeichnungen bzw. Schaltpläne angefertigt werden, wie sie für Häuser, Maschinen oder Elektroanlagen üblich sind.

Die Ignoranten bekommen jetzt die Quittung für ihre Unterlassungen. Mit einem riesigen zeitlichen Aufwand müssen sie Befehl für Befehl ihre Software durchforsten, um festzustellen, wo sie möglicherweise ab dem Jahr 2000 falsche Schlußfolgerungen aus einem gespeicherten Datum ziehen. Manche Berechnungen der Computerindustrie gehen davon aus, daß die Kosten für die „Reparaturarbeiten"

weltweit höher sind als die Gesamtkosten des 2. Weltkrieges. Nun sorgen wir uns sicher nicht um die Überstunden der Programmierer. Vielmehr geht es um die Frage: Wenn die Systeme so schlecht dokumentiert sind, daß die Jahrtausendumstellung mit einem solchen Aufwand und so vielen Risiken behaftet ist, wie groß ist dann die Chance, zur **Aufdeckung von Manipulationen**, anläßlich von Rechtsstreitigkeiten oder zu Beweiszwecken nachträglich, möglicherweise nach Jahren, feststellen zu können, welche Daten zu welchen Zeitpunkten gespeichert waren bzw. welche programmgesteuerten Schlußfolgerungen aus welchen Informationen gezogen worden sind?

Es reicht nicht, resignierend festzustellen, daß die in automatisierten Verfahren eingesetzte Software in der Regel nur bedingt revisionsfähig ist. Aus der Jahr-2000-Problematik sind umgehend **Konsequenzen** zu ziehen. Zuallererst ist die Verantwortung für die Dokumentation der bestehenden informationstechnischen Systeme (Hardware, Software, Datenbestände, Organisationsregelungen) eindeutig festzulegen. Sodann sollten sich alle Aufsichtsbehörden und Behördenleitungen darin einig sein, daß es keine Entschuldigungen für Dokumentationsmängel gibt. Was in allen ingenieurwissenschaftlichen Bereichen als eine bewährte Grundregel angesehen wird, kann im Bereich der automatisierten personenbezogenen Datenverarbeitung nicht falsch sein. Alle nicht hinreichend dokumentierten Systeme sollten mit einem „Verfallsdatum" versehen werden. Ihr Einsatz ist zu stoppen, wenn nicht bis zu dem betreffenden Zeitpunkt eine aussagefähige Dokumentation erstellt worden ist.



Grundsätzlich ist zu bemängeln, daß IT-Systeme nicht in einer Weise geprüft werden, wie selbst die einfachsten elektrischen Geräte. Ein **„Sicherheits-TÜV"** im laufenden Betrieb existiert erst recht nicht. Ohne grundlegende Änderungen wird sich das Jahr-2000-Problem in einigen Jahren als ein „Peanut", im Verhältnis zu den Revisionsdefiziten, die die immer komplexer werdenden Informations- und Verarbeitungssysteme dann aufweisen, darstellen.

Was ist zu tun?
Den IT-Verantwortlichen sollten vom Gesetzgeber bezüglich der Anforderungen an die Innen- und Außentransparenz der Informations- und Verarbeitungssysteme „Daumenschrauben" angelegt werden. Die Novelle zum Landesdatenschutzgesetz gibt hierfür eine gute Chance.

6.2 Paßwortsicherheit – ein unterschätztes Problem

Die meisten Sicherheitskonzepte bauen darauf auf, daß verschlüsselt gespeicherte Paßwörter nicht geknackt werden können. Heute leicht erhältliche Hacker-Software mit komfortabler Benutzeroberfläche stellt dies in Frage. Die Paßwortgestaltung muß überdacht werden.

Man kann ohne Übertreibung feststellen: In den Paßwörtern tickt eine ebenso große **Zeitbombe** wie in den vor etwa 15 Jahren erstmals aufgetretenen Compu-

terviren. Man ging bis vor kurzem nämlich davon aus, daß die von den Computerbetriebssystemen vorgenommenen Verschlüsselungen der Paßwörter mathematisch faktisch nicht zu knacken sind. Fast alle Sicherheitskonzepte bauen deshalb auf folgender Annahme auf: Wer sich selbst ein „gutes" Paßwort vergibt und es nicht verrät, kann sicher sein, daß niemand anders seine EDV-Systeme in Gang setzen, Programme aufrufen oder Datenbestände verändern kann. Weist ein Protokoll aus, daß Frau Müller bzw. Herr Meier eine Abfrage gestartet oder eine Veränderung vorgenommen hat, dann war es diese Person; wer sonst hätte unter der betreffenden (paßwortgesicherten) Kennung arbeiten können?

Diese Konstruktion gerät nun ins Wanken. Seit einiger Zeit sind Programme frei verfügbar, die mit Hilfe großer elektronischer Lexika und geeigneter Entschlüsselungstechnik zu einfach gewählte Paßwörter erkennen. Wessen Paßwort nicht lang und nicht kompliziert genug aufgebaut ist, muß also seit kurzem befürchten, daß andere unter seiner Identität Aktivitäten entfalten, für die er die Verantwortung trägt. Wir haben derartige **Programme** unter „Laborbedingungen" **getestet**: In der Zeit von Freitagabend bis Montagmorgen wurden 2 000 von 2 500 „echten" Paßwörtern (also 80 Prozent) entschlüsselt. Als Ergebnis ist festzustellen, daß Paßwörter mit weniger als sechs Zeichen, die nicht neben Buchstaben auch Ziffern und Sonderzeichen enthalten, zu unsicher sind. Es ist zu erwarten, daß in absehbarer Zeit acht Zeichen als Mindestlänge sicherer Paßwörter gelten wird.

Voraussetzung für das Entschlüsseln codierter Paßwörter ist allerdings der Zugriff auf die Systemdatei der verschlüsselten Paßwörter. Diese Befugnis haben faktisch alle **Systemadministratoren**. Sie werden somit automatisch in den Kreis der Verdächtigen geraten, wenn ein eines Fehlverhaltens verdächtigter Mitarbeiter behauptet, die protokollierten Aktivitäten stammten nicht von ihm (denkbares Szenario: Auf der lokalen Platte eines vernetzten PC, auf die nur ein bestimmter Mitarbeiter Zugriff hat, befinden sich kinderpornographische Daten; die Protokolle weisen aus, daß sie unter seiner Kennung aus dem Internet heruntergeladen worden sind. Niemand wird ihm glauben, daß er die Daten nicht gespeichert hat).

Einige Betriebssysteme gestatteten bisher selbst Systemadministratoren nicht, derartige Aktivitäten manipulativ vorzunehmen. Diese Zeiten sind vorbei. Für viele Betriebssysteme sind Crack-Programme erhältlich. Sie werden daher künftig sogar in den Verdacht geraten können, Dritten die Paßwörter von Vorgesetzten, Mitarbeitern von Personalabteilungen und sonstigen Personen, die vertrauliche Daten zu verarbeiten haben, verraten zu haben. Deshalb müssen sie selbst ein Interesse daran haben, daß Paßwörter so gestaltet werden, daß die jeweils „gängigen" Crack-Programme keine Chance haben. Hierauf haben wir ausführlich in einer **Bekanntmachung im Amtsblatt** hingewiesen (Amtsblatt 1998, S. 688). Die Veröffentlichung finden Sie auch auf unserer Homepage:





www.schleswig-holstein.datenschutz.de
(Rubrik: Informationen speziell für Behörden)

Was ist zu tun?
Im Beisein der IT-Verantwortlichen sollten die Systemadministratoren regelmäßig die „Paßwortgüte" durch Einsatz von Crack-Programmen überprüfen. Kompromittierte Paßwörter sind durch die Benutzer sofort zu ändern.

6.3 Warum gibt es keine Verwaltungsinformatiker?

Die personenbezogene Datenverarbeitung in der öffentlichen Verwaltung unterliegt anderen Rechtsregeln als die in der Wirtschaft. Wer hochkomplexe Informations- und Kommunikationstechnik unter diesen spezifischen Bedingungen sicher und ordnungsgemäß einsetzen will, braucht eine fundierte Ausbildung. Trotzdem verzichtet die Verwaltung bislang darauf, ihren Nachwuchs und ihre potentiellen Führungskräfte entsprechend zu schulen.

Das zu Ende gehende dritte und das beginnende vierte Jahrzehnt des Computereinsatzes ist in Wirtschaft und Verwaltung dadurch gekennzeichnet, daß die hochspezialisierten Rechenzentren immer mehr an Bedeutung verlieren und an ihre Stelle eine Vielzahl unternehmens- und behördenspezifische **dezentrale IT-Organisationseinheiten** treten. Gleichzeitig erweitert sich das Spektrum der durch Informationstechnik unterstützten Arbeitsabläufe. Wurden in den vergangenen Jahren rechenintensive Aufgabenstellungen durch den Computereinsatz rationalisiert, verlagert er sich derzeit hin zum Informations- und Kommunikationsmittel.

Die Anforderungen und Ziele für die nächsten Jahre sind durch Begriffe wie E-Commerce auf der Basis digitaler Signaturen, Workflow-Management im Rahmen nahezu papierloser Verarbeitungsprozesse, individuelle E-Mail-Kommunikation für jedermann über offene, grenzüberschreitende Netze bei gleichzeitiger Gewährleistung der Vertraulichkeit durch allgemein verfügbare Verschlüsselungsverfahren, Data-Warehousing zur Optimierung der Datennutzung und zur Servicesteigerung gegenüber den Kunden gekennzeichnet (vgl. Tz. 7). Speziell in der öffentlichen Verwaltung spricht man von **interaktiven Verwaltungsverfahren** über öffentliche Netze, von einer transparenteren Verwaltung durch einen allgemeinen Informationszugang und von Verwaltung als Angebot von Produkten und Dienstleistungen.

Die Applikationen werden zunehmend anspruchsvoller, die **Technik komplexer** und die Anforderungen an die Verfügbarkeit der Systeme, die Integrität der Verfahren und die Vertraulichkeit der Datenbestände höher.

Die Leistungen dieser Systeme nutzbringend in Anspruch zu nehmen ist die eine Seite, sie zu gestalten und zu beherrschen eine andere. Dies hat die Wirtschaft nicht zuletzt auch aufgrund von Mißerfolgen und den damit verbundenen Imageverlusten sowie Umsatz- und Gewinneinbußen sehr schnell erkannt. Wer den aktuellen Stellenmarkt in den Tageszeitungen studiert, stellt fest, daß die **Berufsbilder** sich ständig verändern. Wer sucht heute noch „schlichte" Programmierer,

Operatoren oder ganz allgemein EDV-Fachleute? Gebraucht werden Entwicklungsprojektleiter, Systemingenieure, Netz- und Systemadministratoren, Datenbankmanager, Objekt-Designer, Systemanalytiker, Organisationsprogrammierer usw. mit jeweils branchenspezifischen Kenntnissen. Dem haben sich die Universitäten und Hochschulen mit ihrem Ausbildungsangebot angepaßt. Wirtschaftsingenieurwesen, theoretische und angewandte Informatik, Wirtschaftsinformatik, Betriebswirtschaft mit Schwerpunkt DV, Kommunikationselektronik usw. sind Studiengänge, die vor wenigen Jahren noch nicht bekannt waren.

Diese Ausdifferenzierung scheint es in der Verwaltung nicht zu geben. Die Universitäten sahen sich bisher nicht veranlaßt, das Jurastudium, das in den meisten Verwaltungsbereichen Voraussetzung für die Übernahme von Managementpositionen ist, um die Komponente „Informatik" zu ergänzen. Desgleichen bilden die Verwaltungsfachhochschulen **keine Verwaltungsinformatiker** aus. Selbst diejenigen Absolventen der schleswig-holsteinischen Verwaltungsfachhochschule, die alle Lehrangebote in Richtung Informatik in Anspruch nehmen, erhalten nicht das erforderliche Rüstzeug, um die Verantwortung für die Konzipierung der IT-Systeme z. B. einer Kreisverwaltung übernehmen zu können. Nahezu alle kleineren und mittleren Organisationseinheiten, mit denen wir im Rahmen unserer Prüfungen Kontakt hatten oder in denen wir beratend tätig wurden, beklagen diesen Mangel. Die **Folgen** sind **fatal**. Mit großem Aufwand erhalten Informatiker eine verwaltungsrechtliche oder Verwaltungsspezialisten eine informationstechnische Nachschulung. Da dies in der Regel als „Training on the Job" geschieht, erzeugt man, es mag überzogen klingen, in beiden Fällen partielle Autodidakten. Das dürfte auf der sachbearbeitenden Ebene noch einige Zeit hinnehmbar sein. Eine systematische Ausbildung ist aber für Mitarbeiter, die Führungsverantwortung übernehmen sollen, unverzichtbar.

Aus dem IT-Gesamtplan der Landesregierung ergibt sich, daß allein das Land jährlich circa **120 Millionen DM** in **IT-Maßnahmen** investiert und über 380 Mitarbeiter mit der Entwicklung und Pflege von Software sowie mit der Administration der technischen Systeme betraut hat. Ein etwa gleichgroßes Volumen dürfte für den Bereich der Kommunen und der sonstigen öffentlichen Stellen im Lande anzusetzen sein. Es ist für die Gewährleistung der Sicherheit und Ordnungsmäßigkeit einer personenbezogenen Datenverarbeitung dieser Größenordnung und „Sensibilität" unabdingbar, daß das Management und die Administration in den Händen speziell und systematisch ausgebildeter Mitarbeiterinnen und Mitarbeiter liegt. Denn offenbar können nur auf diesem Wege die auch in diesem Jahr wieder festgestellten datenschutzrechtlichen Unzulänglichkeiten und Defizite (vgl. z. B. Tz. 6.7) behoben werden. Wir haben erste Kontakte mit der **Verwaltungsfachhochschule** aufgenommen; die entscheidende Initiative wird jedoch von den Behörden kommen müssen.



Was ist zu tun?
Man sollte alle Beteiligten und Interessierten zu einem „runden Tisch" einladen und Schleswig-Holstein auch auf diesem Gebiet zu einem Vorreiter auf dem Weg in die Informations- und Kommunikationsgesellschaft werden lassen.

6.4 Innenministerium läßt sich bezüglich der Gestaltung seiner IT-Services beraten

Auf dem Gebiet der Informations- und Kommunikationstechnik wird der Innenminister mehr und mehr zur Servicestelle für die anderen Ressorts. Die damit verbundenen Zuständigkeits- und Verantwortungsverlagerungen dürfen nicht zu Sicherheitslücken führen. Das Innenministerium läßt sich neuerdings von uns beraten.

In den letzten beiden Tätigkeitsberichten (vgl. 19. TB, Tz. 7.9; 20. TB, Tz. 6.7.6) haben wir darüber berichtet, welche unterschiedlichen Auffassungen zwischen dem Innenministerium und uns bezüglich der datenschutzrechtlichen Bewertung des **CAMPUS-Netzes** bestanden haben. Da sich in den vergangenen Jahren immer mehr bestätigt hat, daß das Innenministerium den anderen Ressorts nicht nur Leitungswege zur Verfügung stellt, sondern ihnen gegenüber mit steigender Tendenz auch sehr spezifische Dienstleistungen erbringt, haben wir keinen Anlaß gesehen, von unserer Forderung nach einer uneingeschränkten Anwendung der Sicherheits- und Ordnungsmäßigkeitskriterien der Datenschutzverordnung abzugehen.

> **?** ***CAMPUS-Netz***
>
> *Das CAMPUS-Netz verbindet die lokalen Rechnernetze der Ministerien, der Staatskanzlei und des Landtages auf der Basis einheitlicher Konventionen. Über eine definierte Schnittstelle ist es mit dem Schleswig-Holstein-Netz der Datenzentrale und darüber wiederum mit dem Internet verbunden. Betreiber des CAMPUS-Netzes ist das Innenministerium.*

Dieser Sicht hat sich der Innenminister nunmehr angeschlossen und uns gebeten, ihn bei der Neugestaltung der Zusammenarbeit der Ressorts auf dem Gebiet der Informationsverarbeitung und der Kommunikation über Netze beratend zu unterstützen. Wir haben eine Arbeitsgruppe aus Mitarbeitern beider Häuser gebildet, die ihre Tätigkeit Ende 1998 aufgenommen hat. Welches Pensum vor ihr liegt, mögen zwei Zahlen verdeutlichen: Der Arbeits- und Terminplan umfaßt insgesamt circa 80 Positionen, an circa 50 Aktivitäten werden wir beteiligt sein. Ein Abschluß des Projektes wird nicht vor Mitte 1999 zu erwarten sein.

Einen unserer wesentlichen Kritikpunkte am CAMPUS-Netz hat der Innenminister zwischenzeitlich aufgegriffen. Die von der Datenzentrale als externem Dienstleister konzipierte und betriebene **Schnittstelle zum Internet** (die sogenannte Firewall) ist inzwischen von unabhängigen Dritten getestet worden. Das Gutachten ist uns kurz vor Redaktionsschluß dieses Berichtes zugegangen. Wir werden es analysieren und die Ergebnisse in die Sicherheitsüberlegungen einfließen lassen.

6.5 Noch keine konkreten Fortschritte beim Schleswig-Holstein-Netz der Datenzentrale

Als die Datenzentrale ihren Rechenzentrumsbetrieb in Altenholz aufnahm, hat sie ihre Kunden und Besucher selbstverständlich eingehend über ihre Arbeit und die getroffenen Sicherheitsmaßnahmen informiert. Es ist nicht nachzuvollziehen, warum sie in ihrer neuen Rolle als Kommunikationsdienstleister (Provider) so wenig auf Transparenz und Sicherheit bedacht ist.

Seit drei Jahren üben wir Kritik an den vertraglichen Vereinbarungen zwischen der Datenzentrale und ihren Kunden, soweit sie das **Schleswig-Holstein-Netz** zur Kommunikation untereinander, mit dem Rechenzentrum der Datenzentrale oder mit dem Internet benutzen. Außerdem sind unseres Erachtens von der Datenzentrale die Bestimmungen der Datenschutzverordnung über den Test, die Freigabe und die Dokumentation dieser Systeme nicht hinreichend beachtet worden (vgl. 19. TB, Tz. 7.8; 20. TB, Tz. 6.7.7).

> ? *Schleswig-Holstein-Netz*
>
> *Das Schleswig-Holstein-Netz ist ein Dienstleistungsangebot der Datenzentrale. Es umfaßt die „Vermietung von Leitungen", die Vernetzung von Behörden, die Verknüpfung mit dem Internet, den Betrieb einer Firewall und vieles andere mehr.*

Im Verlaufe des Jahres sind zwar wieder mehrere Gespräche geführt worden; konkrete Fortschritte hat es aber nicht gegeben. Allerdings konnte in einem „Chefgespräch" am Jahresende vereinbart werden, daß von einer „**Task Force**", bestehend aus dem Datenschutzbeauftragten der Datenzentrale und einem Mitarbeiter unserer Dienststelle, detaillierte Lösungsvorschläge erarbeitet und Zeitpläne aufgestellt werden, deren Umsetzung vom Vorstand der Datenzentrale direkt überwacht werden soll. Es ist zu hoffen, daß im nächsten Tätigkeitsbericht von einem positiven Abschluß der Arbeiten gesprochen werden kann.

6.6 Datensicherheit à la EU – wenn es ums Geld geht II

Wenn es ums Geld geht, wird auch für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung viel getan. Die EU hat der Landwirtschaftsverwaltung drastische Sicherheitsvorschriften verordnet. Die Behörden setzen sie klaglos um, weil sie sonst viele Subventionen verlieren können. Den Datenschützern soll es recht sein.

Im letzten Jahr (vgl. 20. TB, Tz. 6.7.2) haben wir anhand der Test- und Freigabeprozedur des **Landesbesoldungsamtes** dargestellt, daß Behörden sehr wohl in der Lage sind, ihre automatisierten Verfahren zur personenbezogenen Datenverarbeitung sicher zu gestalten. Sie brauchen lediglich die richtige Motivation. Im Hinblick auf die hohen Geldbeträge, die im Rahmen der Berechnung und „Zahlbarmachung" der Gehälter, Löhne, Versorgungs- und Beihilfeleistungen monatlich bewegt werden, ist es für das Landesbesoldungsamt eine Selbstverständlichkeit,

alle Änderungen an den Berechnungsprogrammen sorgfältig zu prüfen, bevor man in die Produktion geht. Auch die Arbeit der Datenzentrale, die als externer Dienstleister unterstützend tätig ist, wird penibel überwacht. Die datenschutzrechtlichen Anforderungen, die man anderenorts als völlig überzogen ansieht, werden hier „mit links" erfüllt, weil es eben ums Geld geht.

Wie die Motivlage sich gleicht: Weil es auch bei der Verteilung der **EU-Mittel** des gemeinsamen **Agrarmarktes** um viele Milliarden Euro geht, hat die Generaldirektion VI der Europäischen Kommission den sogenannten Zahlstellen (in Schleswig-Holstein ist Zahlstelle das Ministerium für ländliche Räume, Landwirtschaft, Ernährung und Tourismus) ein **Sicherheitskonzept** auferlegt, das jedem Datenschutzlehrbuch zur Ehre gereichen würde. Wenn eine Zahlstelle dieses Sicherheitskonzept nicht realisiert, muß sie bei eventuellen Fehlern oder Versäumnissen ohne nähere Prüfung der Ursachen zuviel ausgezahlte Beträge an die EU zurückzahlen. Ein Abweichen vom vorgeschriebenen Sicherheitsstandard wird als „schuldhaftes" Handeln angesehen. Dieser Standard hat es in sich. Ein Auszug:

- Die EDV-Strategie ist von der Behördenleitung zu entwickeln, zu aktualisieren, zu genehmigen und zu lenken.
- Auf dieser Basis sind die Standards und Verfahren festzulegen.
- Die Datensicherheitsstatistik hat zu gewährleisten, daß die Informationen in bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit eingeordnet werden.
- Das Management hat für eine angemessene funktionale Abgrenzung zwischen den EDV- und den Anwenderbereichen zu sorgen.
- Eine unabhängige interne Prüfstelle muß eine ausreichende Fachkompetenz und Authorität besitzen, um EDV-Kontrollen durchzuführen, zu dokumentieren und Verbesserungsvorschläge zu machen.
- Dezidierte Anforderungen werden an die Zutritts- und Zugriffssicherungen, die Systementwicklung, Programmierung und Wartung, die Produktionsumgebung, die Datenfernübertragung und die Notfallvorsorge gestellt.

Das **IT-Referat** des **Landwirtschaftsministeriums** hat zur Umsetzung dieser Anforderungen eine Projektgruppe gebildet und läßt sich von uns beraten. Dabei erwies sich der durch die EU-Vorschriften ausgelöste Schock als heilsam. Bekannte Schwachstellen, deren Behebung unter dem Druck des Tagesgeschäftes bisher immer wieder verschoben worden waren, werden wohl nun endlich ausgemerzt – weil es eben ums Geld geht.

6.7. Kontrollen im Bereich der automatisierten Datenverarbeitung

6.7.1 Hier ist ein Computer – nun nutzt ihn mal schön!

Die Sicherheitsmaßnahmen für Informations- und Kommunikationssysteme, mit denen Sozialdaten verarbeitet werden, müssen besonders wirksam sein. Wer ein Netzwerk mit mehr als 2 500 Arbeitsplätzen in die „Produktion" gehen läßt, ohne ein präzises technisches und organisatorisches Regelwerk wirksam werden zu lassen, handelt fahrlässig.

Neben den unter Textziffer 4.7.2 dargestellten Mängeln in bezug auf die Wahrung des Sozialgeheimnisses wurden im Rahmen der Querschnittsprüfung bei der **AOK Schleswig-Holstein** auch erhebliche Sicherheitsdefizite beim Einsatz der Computersysteme festgestellt.

Die Ausgangslage glich der in der „papierenen Welt". Im Oktober 1996 hat die Direktionsabteilung „Organisationsentwicklung" vom Vorstand der AOK per Dienstanweisung den Auftrag erhalten, den Umgang mit den PC in einer speziellen PC-Dienstanweisung zu regeln. Bis zum September 1998, also im Verlaufe von zwei Jahren, ist jedoch diesbezüglich nichts geschehen. Es gab zum Zeitpunkt der Prüfung weder schriftliche Anweisungen noch Standards, obwohl zwischenzeitlich circa **2 500 Arbeitsplätze mit vernetzten PC** ausgerüstet worden waren. Dementsprechend fanden wir zum Beispiel folgende Gegebenheiten vor:

- Alle Arbeitsplatzrechner waren mit einer **umfassenden Bürokommunikationssoftware** ausgestattet. Nahezu allen Mitarbeitern standen damit die Funktionalitäten „Textbearbeitung", „Präsentationsgrafik", „Tabellenkalkulation", „Datenbankgenerator" und „Mail-System" zur Verfügung. Ihnen waren jedoch keine Weisungen erteilt worden, zu welchen Zwecken die umfangreichen Softwarepakete benutzt werden sollten. Es konnte zum Beispiel nicht geklärt werden, aus welchen Gründen an allen Arbeitsplätzen ein Datenbankgenerator verfügbar sein mußte.
- Eine systematische und umfassende **Schulung** zur Benutzung der Softwarepakete war nicht durchgeführt worden. Auch den Vorgesetzten war der Sinn und Zweck der Installation nicht nahegebracht worden.
- Faktisch konnte jeder Mitarbeiter mit den Programmen verfahren, wie er es für richtig hielt. **Kontrollmöglichkeiten** durch Vorgesetzte bestanden nicht.
- Einige Geschäftsstellenleiter gingen davon aus, daß mit Hilfe des Mail-Systems keine Sozialdaten übermittelt würden, sicher war man sich aber nicht. Bei Stichproben sind tatsächlich **personenbezogene Sozialdaten** gefunden worden. Wie derartige Dokumente gegen unbefugte Zugriffe zu schützen sind und wie zu gewährleisten ist, daß sie ihren Niederschlag in den betreffenden Vorgängen finden, war nicht geregelt.
- Die EDV-Sachbearbeiter in den Geschäftsstellen haben **keine aufgabenspezifische Schulung** erhalten. Das gleiche gilt für die Datenschutzverantwortlichen

in den einzelnen Geschäftsstellen. Beiden Mitarbeitergruppen stellte sich nach dem im Rahmen der Prüfung gewonnenen Eindruck das Gesamtsystem als eine „Black Box" dar.

- Ein **Zugriffskonzept** und eine für Dritte nachvollziehbare Darstellung der technisch realisierten Zugriffsberechtigungen auf die zentralen Verfahren (vgl. Tz. 4.7.2) konnten nicht vorgelegt werden. Mehrfach wurde von den Verantwortlichen eingeräumt, daß dies ein seit langem bekannter Mangel sei. Es sei nicht zu bestreiten, daß viele Zugriffsberechtigungen zu weitgehend seien.
- Weiterhin fehlten Regelungen zur **Löschung** von Datenbeständen, die mit Hilfe der Bürokommunikationssoftware erstellt worden waren. Die Mitarbeiter entschieden selbst, wie lange welche Daten gespeichert blieben. Vorgesetzte hatten faktisch keine Möglichkeit, die Speicherdauer zu kontrollieren, da sie hierfür die Kennung der Mitarbeiter hätten benutzen müssen.
- **Sicherheitskonzepte**, Verfahrensdokumentationen sowie Test- und Freigabeunterlagen konnten weder von der zuständigen Abteilung der Direktion noch von einer der Geschäftsstellen vorgelegt werden.
- **Dateibeschreibungen** sind nur für die Datenbestände, die im Rahmen der zentralen Verfahren geführt werden, erstellt worden, nicht für Datenbestände, die mit Hilfe der Bürokommunikationssoftware aufgebaut worden sind.
- **Geräteverzeichnisse** gemäß den Anforderungen des Landesdatenschutzgesetzes konnten nicht vorgelegt werden.

Die von uns beanstandeten Defizite waren dem Vorstand aufgrund der Berichte der eigenen Sozialdatenschutzbeauftragten bekannt. Für Abhilfe war nicht gesorgt worden, so daß wir hierüber das Ministerium für Arbeit, Gesundheit und Soziales als die zuständige Aufsichtsbehörde unterrichtet haben. Unsere Beanstandungen hat die AOK ausnahmslos als berechtigt akzeptiert. Sie beabsichtigt, sie im Rahmen der unter Textziffer 4.7.2 dargestellten Vorgehensweise zu beheben. Ein Abschluß der Arbeiten soll ebenfalls bis Ende September 1999 erreicht sein.

Was ist zu tun?
Die AOK wird ein neues Grundverständnis für den Technikeinsatz im Sozialleistungsbereich entwickeln müssen. Die Verantwortlichen werden die Maxime „Was nicht genehmigt ist, darf auch nicht möglich sein" technisch und organisatorisch umsetzen müssen.

6.7.2 Wer trägt die Verantwortung für den Computereinsatz in den Finanzämtern?

Das weitgehend automatisiert ablaufende Besteuerungsverfahren verlagert sich schrittweise von der „Rechenzentrale" in der Oberfinanzdirektion zurück in die Finanzämter. Die damit verbundenen Schnittstellen- und Sicherheitsprobleme sind bisher unzureichend gelöst worden.

Bis vor wenigen Jahren wurden die 20 Finanzämter im Lande in informationstechnischer Hinsicht von der Oberfinanzdirektion quasi am Gängelband geführt. Ihre gesamte **Hardware- und Softwareausstattung** wurde zentral von Kiel aus verwaltet. Die Vorsteher der Finanzämter hatten nur dafür zu sorgen, daß ihre Steuerfachleute das notwendige EDV-Wissen hatten, um auf den Vordrucken bzw. Bildschirmmasken die richtigen Werte in die richtigen Kästchen zu übertragen. Alle Aspekte der Sicherheit und Ordnungsmäßigkeit der sich an die Erfassung anschließenden automatisierten Verarbeitung der Daten waren von den hierfür zuständigen Referaten in der Oberfinanzdirektion mit insgesamt mehr als 150 Mitarbeitern zu lösen.

Diese sehr einfache **Organisationsstruktur** hat sich zwischenzeitlich entscheidend **geändert**. In dem Maße, wie die Verarbeitungsprozesse aus der „Rechenzentrale" in die Finanzämter zurückverlagert wurden, mußten ihnen auch eigene Zuständigkeiten übertragen werden. Wie sich in der bereits unter Textziffer 4.10.4 angesprochenen sicherheitstechnischen Überprüfung eines Finanzamtes zeigte, ist die Synchronisation der Schnittstellen zwischen den Verantwortungsbereichen der Finanzämter und denen der Oberfinanzdirektion bisher noch nicht so gelungen, wie es im Hinblick auf die Sensibilität der verarbeiteten Daten als erforderlich und angemessen anzusehen wäre.

Zunächst muß man sich die **Größenordnungen** vor Augen führen. In dem betreffenden Finanzamt waren fünf Rechnersysteme mit insgesamt sieben Betriebssystemen bzw. betriebssystemähnlichen Komponenten installiert. Circa 190 Arbeitsplatzsysteme waren direkt mit den Zentralrechnern in der Oberfinanzdirektion bzw. in der Datenzentrale verbunden. Über 100 weitere Arbeitsplatzrechner (PC) waren mit den Rechnersystemen im Finanzamt vernetzt. Circa 80 Mitarbeiter benutzten für ihre Arbeit Einzelplatzsysteme, teilweise in der Form von Notebooks im Außendienst.

Für den reibungslosen Ablauf der automatisierten Datenverarbeitung im Finanzamt waren vier Personen zuständig. Die wesentlichen **Administrationsfunktionen** wurden allerdings von Mitarbeitern der Oberfinanzdirektion gelegentlich vor Ort, in der Regel jedoch im Wege der **Fernwartung** durchgeführt. Hierbei waren folgende Schwachstellen zu beanstanden:

- In der Oberfinanzdirektion erfolgte die Administration durch 16 Mitarbeiter, die alle die gleiche Benutzerkennung und das gleiche Paßwort benutzten. Alle verfügten über einen uneingeschränkten Zugriff auf die IT-Systeme und Datei-

en in den Finanzämtern. Diese **Verfahrensweise** muß unter Sicherheitsaspekten als „**riskant**" eingestuft werden. Ein Gruppenpaßwort ist nach allen Erfahrungen nicht lange geheimzuhalten. Außerdem kann nicht protokolliert werden, welche Aktivitäten von welchem Mitarbeiter zu verantworten sind.

- Daneben war noch eine größere Anzahl von sogenannten **File-Administratoren** tätig. Eine Dokumentation über deren Befugnisse und Zugriffsberechtigungen konnte nicht vorgelegt werden.
- Die Administration der IT-Systeme des Finanzamtes durch Mitarbeiter der Oberfinanzdirektion wurde nicht protokolliert und systematisch überwacht. Das Finanzamt war in der Regel über die Aktivitäten nicht informiert. Eine **unbefugte Kenntnisnahme** von Steuer- oder Personaldaten durch Administratoren wäre also nicht nachzuvollziehen gewesen.
- Den Mitarbeitern des Finanzamtes war es gestattet, Datenbestände anzulegen, auf die die Vorgesetzten **keine unmittelbaren Zugriffsmöglichkeiten** hatten. Welche Steuer- oder Personaldaten in diesen Dateien wie lange gespeichert wurden, hätten die Sachgebietsleiter nur im Beisein der Mitarbeiter überprüfen können. Deshalb ist auf derartige Kontrollen bislang verzichtet worden. In die papierene Welt übertragen, würde dieser Zustand dem Führen von „schwarzen" Akten entsprechen.
- Die Zugriffsberechtigungen für die Mitarbeiter des Finanzamtes wurden zentral von der Oberfinanzdirektion vergeben. Eine **Dokumentation** der Rechtevergabe konnte vom Finanzamt **nicht vorgelegt** werden. Die Verantwortlichen im Finanzamt konnten mithin nicht überprüfen, ob die von ihnen gewollten Befugnisse bzw. Beschränkungen auch tatsächlich realisiert worden sind.

Aufgrund der bereichsspezifischen Regelungen im Finanzverwaltungsgesetz ist die Steuerverwaltung recht frei in der Entscheidung, wo sie die Zuständigkeitsgrenzen zwischen den Finanzämtern und der Oberfinanzdirektion zieht. Dies darf aber nicht dazu führen, daß die Verantwortlichkeiten für die Handhabung der technischen Systeme und für die Wahrung des Steuergeheimnisses in den einzelnen Datenverarbeitungsabschnitten verschwimmen. Das Finanzamt hat – wie zu erwarten – darauf verwiesen, daß diese Probleme in die **Zuständigkeit der Oberfinanzdirektion** fallen. Diese hat unseren Beanstandungen nicht widersprochen und eine Behebung der Mängel zugesagt. Konkrete Ergebnisse lagen bis zum Ende des Berichtszeitraumes noch nicht vor. Es besteht die Absicht, sich von uns beraten zu lassen.

Was ist zu tun?
Die Dezentralisierung der Verarbeitungsprozesse in der Steuerverwaltung muß von aufbau- und ablauforganisatorischen Maßnahmen begleitet werden, die die Sicherheit und Ordnungsmäßigkeit gewährleisten und die jeweiligen Verantwortlichkeiten transparent machen.

6.7.3 Computer im Krankenhaus – keiner weiß, wo es lang geht

Von den Verantwortlichen eines großen Krankenhauses muß man ein besonderes Sicherheitsbewußtsein und Durchsetzungsvermögen bei der Umsetzung der gesetzlichen Vorschriften erwarten. Ein weiteres Mal hat eine Prüfung gezeigt, daß zwischen den berechtigten Ansprüchen der Patienten und den konkreten Maßnahmen der Ärzte und Verwaltungschefs große Lücken klaffen.

Wer sich in ein Krankenhaus begibt, ist in der Regel mit so vielen Sorgen um seine Gesundheit belastet, daß er bei seinen Gesprächen mit den Mitarbeitern der Krankenhausverwaltung, den Schwestern und Pflegern, den Ärzten usw. nicht mit erhöhter Aufmerksamkeit darauf achtet, daß sein informationelles Selbstbestimmungsrecht bei der Verarbeitung seiner höchst **sensiblen personenbezogenen Daten** gewahrt wird. Mit Recht wird er davon ausgehen, daß das Krankenhaus nicht nur alles tut, um ihm eine optimale Behandlung angedeihen zu lassen, sondern die dabei anfallenden Informationen auch höchst sorgsam und vertraulich behandelt. Die Wahrung des Patientengeheimnisses gehört zu den Qualitätsstandards, die bei einem guten Krankenhaus vorausgesetzt werden können.

Damit diesem Anspruch in der Praxis Rechnung getragen wird, richten wir seit Jahren unser Augenmerk in besonderem Maße auf die personenbezogene Datenverarbeitung in Krankenhäusern (vgl. z. B. 16. TB, Tz. 6.6.4; 17. TB, Tz. 6.6.2; 18. TB, Tz. 4.8.3; 19. TB, Tz. 6.6.2; 20. TB, Tz. 4.8.1 und Tz. 6.7.1).

Bei all diesen Prüfungen haben wir feststellen müssen, daß es mit der Sorgfalt beim Umgang mit den Patientendaten nicht zum Besten bestellt ist. Das gilt nicht nur für die „papierene Welt" der Patientenakten, sondern besonders auch für den Computereinsatz. Das **Städtische Krankenhaus in Kiel** machte hiervon keine Ausnahme. Das Krankenaktenarchiv war zwar straffer organisiert, als wir es in anderen Krankenhäusern angetroffen haben, aber die Unzulänglichkeiten in bezug auf die Sicherheit und Ordnungsmäßigkeit der automatisierten Datenverarbeitung müßten aber jedem Patienten die Zornesröte ins Gesicht steigen lassen. Einige von uns beanstandete Sachverhalte mögen dies verdeutlichen:

- Konzepte für die Gestaltung der automatisierten Patientendatenverarbeitung, **Sicherheitskonzepte**, Dienstanweisungen für die Administratoren und die Benutzer usw. lagen nicht vor.
- Es fehlte eine **Dokumentation** über die **Zugriffsrechte** der einzelnen Mitarbeiter. Die Rechte wurden von den EDV-Stellen vergeben, ohne daß die Fachabteilungen beteiligt waren.
- Die vielfältigen **Verfahren** waren **nicht** so **dokumentiert**, daß sie für außenstehende Fachleute nachvollziehbar waren.
- Die Arbeiten der **Systemadministratoren** wurden nicht protokolliert.
- Die Befugnisse **externer Fernwartungsunternehmen** waren nicht vertraglich

geregelt, ihre Arbeiten wurden nicht hinreichend überwacht.

- Alle Arztbriefe, Befundberichte usw. wurden in Form von **Textdokumenten** seit Jahren außerhalb der Patientenakten elektronisch gespeichert. Dies geschah nicht, um den Ärzten die Anamnese zu erleichtern, sondern um für den Fall, daß in den nächsten Jahren digitale Patientenakten eingeführt würden, einen Ausgangsbestand zu besitzen. Über Zuordnungs-, Aktualitäts- und Richtigkeitsprobleme machte man sich aber keine Gedanken. Wenn sie auch nicht auf alle Datensätze zugreifen konnten, so verfügten die Mitarbeiterinnen und Mitarbeiter des ärztlichen Schreibdienstes doch auf diese Weise über den umfassendsten Überblick über die Patientendaten im ganzen Krankenhaus. Es ist zu hoffen, daß ihr Pflichtbewußtsein sie daran gehindert hat, von ihren Zugriffsmöglichkeiten Gebrauch zu machen.
- „Selbstverständlich" konnten die meisten Mitarbeiter auf ihren PC **eigene Datenbestände** anlegen, auf die die leitenden Ärzte, Vorgesetzte usw. keinen Zugriff hatten. Auch hier macht ein Vergleich mit der papierenen Welt die Brisanz deutlich: Wer würde einem ärztlichen Mitarbeiter die Führung „schwarzer" Patientenkarteien gestatten?
- Obwohl man einen absoluten Diebstahlschutz für PC in einem so großen Krankenhausbetrieb nicht realisieren kann, wurden bei vielen PC personenbezogene Daten auf der lokalen Festplatte abgelegt. Sein schlechtes Gewissen wegen dieses Sicherheitsrisikos beruhigte ein Mitarbeiter dadurch, daß er seinen PC mit einem Stahlseil **am Heizungsrohr angekettet** hatte, seitdem nebenan zwei PC gestohlen worden waren.

Die Sicherheitsproblematik wird dadurch gesteigert, daß von verschiedenen Abteilungen in eigener Verantwortung praktisch **vier voneinander unabhängige Informationssysteme** entwickelt und betrieben werden. Es sind dies die Verwaltung, das Zentrallabor, die Radiologie und die II. Medizinische Klinik, die durch ein unklares Vertragsverhältnis zwischen der Stadt Kiel und der Christian-Albrechts-Universität zu Kiel in das Städtische Krankenhaus „eingebettet" ist. Eine Koordination dieser vier Datenverarbeitungsinseln besteht nicht. Die daraus resultierenden Defizite werden von den Fachbereichen durchaus gesehen. Dies wird exemplarisch aus den nachfolgenden **Aussagen des Direktors** der **II. Medizinischen Klinik** deutlich (Zitate):

- Fast alle Beanstandungen beruhen auf tatsächlichen Defiziten im IT-Bereich der Abteilung. Die angemahnten Veränderungen erscheinen im Interesse einer optimalen Datensicherheit berechtigt.
- Warum die Arztbriefschreibung in der II. Medizinischen Klinik in einem gesonderten Verfahren abläuft, ist auch uns nicht klar.
- Die PC der Mitarbeiter sind „frei" nutzbar, weil sie aus Mitteln für Forschungszwecke beschafft worden sind und auch hierfür genutzt werden.
- Eine sachgerechte Regelung der IT-Aufgaben ist mit den zur Zeit vorhandenen Mitarbeitern schon allein aufgrund der fehlenden Qualifikation nicht möglich. Der Umfang der durchzuführenden Maßnahmen zur Datensicherheit setzt

zusätzliches Personal voraus.

- Die Protokollierung der Aktivitäten der Systembetreuer kann mit dem vorhandenen Personal nicht gewährleistet werden.
- Die Entwicklung eines an den Bedürfnissen der Klinik orientierten IT-Konzeptes wird als dringend erforderlich angesehen, um eine hinreichende Datensicherheit zu gewährleisten.
- Die Einhaltung der datenschutzrechtlichen Bestimmungen im Klinikbereich fällt eindeutig in den Verantwortungsbereich der Ärzte. Die Situation stellt sich so dar, daß zwar die Verpflichtung zur Erteilung entsprechender Anordnungen eindeutig gegeben ist, jedoch niemand vorhanden ist, der diese Anordnungen ausführen kann, da entsprechend qualifiziertes Personal lediglich im Bereich der Klinikverwaltung vorhanden ist. Wir sehen in dieser Situation ein Dilemma, das keiner einfachen Lösung zugänglich ist.

Die **Stadt Kiel** als verantwortlicher Träger des Krankenhauses hat uns diese Ausführungen kommentarlos übersandt. Offenbar teilt sie diese Auffassungen. Unserer Kritik an den Verhältnissen in den anderen Bereichen des Städtischen Krankenhauses hat sie ebenfalls nicht widersprochen und darauf verwiesen, daß der Gesamtkomplex der personenbezogenen Informationsverarbeitung in den nächsten Jahren neu gestaltet werden soll. Hierbei will sie sich durch uns beraten lassen. Als Termin für erste Gespräche ist uns das 1. Halbjahr 1999 genannt worden.

Was ist zu tun?
Die Stadt Kiel muß die personenbezogene Datenverarbeitung in ihrem Krankenhaus dringend „auf Vordermann" bringen. Nicht die „Bauchschmerzen" der Mitarbeiter und Manager des Krankenhauses, sondern die der Patienten, d. h. ihr Interesse an der Wahrung des Patientengeheimnisses, müssen das Handeln bestimmen.

7. Neue Medien und Informationstechniken

7.1 Internet

7.1.1 Anonymer Internet-Zugang

Es gibt leistungsfähige Methoden, anonym im Internet zu surfen, z. B. mit Hilfe sogenannte Mix-Systeme. Zur Zeit wird in unserer Dienststelle ein Prototyp der Technischen Universität Dresden weiterentwickelt, um einen anonymen Zugriff auf Internet-Angebote von Beratungsstellen anbieten zu können.

Beim Surfen im Internet hinterläßt jeder Nutzer **Datenspuren**, z. B. welche Webseite wie lange betrachtet wurde, welcher Weg durch das Angebot gewählt wurde usw. Daraus lassen sich die Interessen und das Kommunikationsverhalten des Nutzers ableiten, selbst wenn die Informationen nicht immer unmittelbar personenbezogen sind. Während es in der Welt außerhalb des Internet noch viele Bereiche gibt, in denen Anonymität zugelassen oder gewollt ist, z. B. beim Einkaufen oder beim Aufsuchen von Beratungsstellen, kann man sich im Internet nicht darauf verlassen: Jeder „Schaufensterbummel" durchs Internet läßt sich auswerten.

Die Medizinische Universität zu Lübeck (MUL) wandte sich an uns, weil dort das **Beratungsangebot „Ecstasy Online"** aufgebaut wird. Da die herkömmliche Drogenberatung von Kindern und Jugendlichen nicht genügend angenommen wird, versucht man, diese Zielgruppe per Internet zu erreichen. Dabei ist allerdings von großer Bedeutung, daß durch anonyme Abrufmöglichkeiten ein Vertrauensverhältnis geschaffen werden kann.

Auf der letzten CeBIT wurde ein leistungsfähiger **Mix-Prototyp** der TU Dresden vorgestellt, der Anonymität beim Webzugriff gewährleisten kann. Wir haben die Entwickler mit Vertretern der MUL zusammengebracht. Leider ist die notwendige Weiterentwicklung des Prototyps in Dresden aus finanziellen Gründen nicht möglich. Das Projekt ist jedoch von sehr großer Bedeutung nicht nur für die MUL, sondern für alle Bereiche, in denen eine anonyme Nutzung im Internet notwendig oder zumindest wünschenswert ist. In den Multimediagesetzen wird sogar gefordert, daß eine Inanspruchnahme von Diensten, soweit technisch möglich und zumutbar, anonym oder unter Pseudonym angeboten wird (vgl. 20. TB, Tz. 7.1).

? ***Mix-System***

Ein Mix-System besteht aus mehreren Stationen (Mixe), über die Nachrichten geschickt werden. Jeder Mix sammelt die eingehenden Nachrichten, sortiert sie um und sendet sie nach einer gewissen Zeit weiter. Damit kann kein Zusammenhang zwischen den eingehenden und den ausgehenden Nachrichten hergestellt werden. Die gesamte Kommunikation läuft verschlüsselt ab. Wenn auch nur ein einziger Mix vertrauenswürdig arbeitet, ist das ganze System vertrauenswürdig, d. h. der Nutzer bleibt anonym.



Diese datenschutzfreundliche Technologie der Mixe soll nun in Schleswig-Holstein für die Praxis weiterentwickelt werden. Im Rahmen der **Landesinitiative Informationsgesellschaft** wurde inzwischen eine Förderung des Modellprojekts beschlossen. Wir werden über seinen Fortgang berichten.

Was ist zu tun?
Auch die Provider von Multimediadiensten müssen – wie rechtlich vorgeschrieben – die Nutzung von Diensten anonym oder unter Pseudonym anbieten.

7.1.2 Möglichst sicher durch das Internet

Wer sich ins Internet begibt, kommt zwar nicht darin um, aber er setzt seinen Rechner und die darauf gespeicherten Daten der Gefahr eines Angriffs aus. Vielen Behörden ist das Risiko nicht bewußt, oder sie wissen nicht, wie sie sich schützen können. Zumindest wenn es um personenbezogene Daten geht, müssen die erforderlichen Sicherheitsmaßnahmen getroffen werden.

Die Fachpresse berichtet regelmäßig von **spektakulären Internet-Angriffen**, z. B. von Packet Sniffern (Ausspähen von übertragenen Daten, auch von Paßwörtern), IP-Spoofing (Fälschen der Rechneradresse, um den Datenverkehr für andere auf den eigenen Computer umzulenken), Telnet Hijacking („Entführen" und Übernehmen von Telnet-Verbindungen), bösartigen ActiveX-Controls oder Viren, wodurch ein Angreifer unter Umständen sogar die vollständige Kontrolle über die Computernutzung erlangen kann. Das Internet an sich ist nicht böse, doch vielfach sind die Angriffe recht simpel ohne viel Expertenwissen zu bewerkstelligen, und unter den etwa 100 Millionen Internet-Nutzern befinden sich auch Spielkinder, Crashkids und bezahlte Spione.

> **?** ***Firewall***
>
> *Eine Firewall (deutsch: „Brandschutzmauer") ist ein System aus Hard- und Software, das nach bestimmten Regeln unerwünschte Kommunikation ausfiltert. Firewalls eignen sich dazu, Netze unterschiedlichen Schutzbedarfs kontrolliert zu verbinden, z. B. für den Anschluß eines LANs ans Internet. Man unterscheidet Paketfilter, die auf Transportebene nach Rechneradresse und Dienst (IP-Adresse und Port) filtern, und Application Level Gateways, die auf Anwendungsebene dienstspezifisch agieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt für einen mittleren Schutzbedarf den Einsatz von kombinierten Systemen.*

Beim Anschluß ans Internet muß man sich darüber im klaren sein, daß der eigene Rechner vom Internet aus erreichbar wird und Angriffen ausgesetzt sein kann. Kein Verwaltungssystem mit personenbezogenen Daten darf deshalb ungeschützt mit dem Internet verbunden sein (vgl. 20. TB, Tz. 7.5.1). Eine einfache Möglichkeit besteht darin, eine Einzelplatzlösung zu realisieren, bei der ein Internet-Zugang über ein physikalisch vom Verwaltungsnetz abgeschottetes Rechner-

system ermöglicht wird, auf dem keine schützenswerten Daten verarbeitet werden. Sobald jedoch eine Öffnung vom Verwaltungsnetz zum Internet geschaffen wird, muß diese Schnittstelle abgesichert werden, z. B. durch eine korrekt installierte und stets gewartete Firewall.

Um die Filterregeln, die die Firewall umsetzen soll, aufzustellen, muß man zunächst in einer **Kommunikationsanalyse** ermitteln, welche elektronischen (Internet-)Dienste von wem genutzt werden sollen. Im Einklang mit einem definierten Sicherheitskonzept und der Security Policy für die Firewall formuliert man unter Einbeziehung aller Beteiligten, insbesondere des internen Datenschutzbeauftragten und des Personalrats, die Regeln und die zusätzlich erforderlichen organisatorischen und technischen Maßnahmen. Diese Planungsphase darf nicht vernachlässigt werden, da aus einer unsauberen oder unbefriedigenden Konzeption Sicherheitseinbußen resultieren.

> ***? Security Policy***
>
> *Die Security Policy (auch Sicherheitspolitik, Sicherheitsrichtlinien) beschreibt die Maßnahmen, die für einen sicheren Aufbau und Betrieb einer Firewall zu treffen sind. Dazu gehört beispielsweise, welche Internet-Dienste für welche Benutzer oder Rechner zugelassen sein sollen. Außerdem werden dort Anforderungen an Organisation, Wartung, Protokollierung und Notfallmanagement formuliert. Die Security Policy muß in das Sicherheitskonzept der Dienststelle eingebettet sein.*

Nach der Auswahl und Installation des Systems muß es vor dem Echtbetrieb, aber auch später bei Konfigurationsänderungen oder bei Bekanntwerden neuer Angriffsmethoden getestet werden. Dabei können **automatisierte Prüfwerkzeuge** helfen. Auch muß ein Verfahren gefunden werden, das die Umgehung der Firewall durch andere Zugänge verhindert. Die beste Firewall hilft nämlich nichts, wenn im zu schützenden Netz auch nur ein Modem mit einem ungesicherten Zugang steht: Selbst eine kurzzeitige Nutzung von Online-Diensten oder Fernwartungszugängen läßt sich in vielen Fällen mißbrauchen, um an der Firewall vorbei Angriffe zu starten.

Der Betrieb und die **Wartung von Firewall-Systemen** sind zeitaufwendig, da nicht nur täglich Protokolldaten ausgewertet werden müssen, um Angriffe erkennen zu können, sondern auch stets Meldungen über Sicherheitslücken und Schutzmaßnahmen auszuwerten und die Systeme gegebenenfalls anzupassen sind. Die Mitarbeiter, die Firewalls aufbauen und betreiben sollen, benötigen eine Menge Know-how, um Angriffe erkennen und richtig reagieren zu können.

Leider bieten auch Firewalls keine 100%ige Sicherheit. Man kann aber ein akzeptabel hohes Maß erreichen, wenn man die folgenden **Grundregeln** beachtet:

- Die Firewall stellt den alleinigen Zugang zum Internet dar.
- Die Firewall wird nicht für weitere Aufgaben (z. B. als File- oder Mail-Server) genutzt.

- Die Firewall baut auf einer definierten Security Policy auf und setzt diese um.
- Konzeption, Aufbau und Betrieb erfolgen durch geeignetes und geschultes Personal.
- Es werden genügend Ressourcen (Zeit und Geld) eingeplant.
- Die Firewall-Administration wird über einen gesicherten Zugang realisiert.

Weitere **Sicherheitsmechanismen** wie Verschlüsselung, digitale Signatur und Virenschutzsysteme sind auch für die Einzelplatzlösungen mit Internet-Zugang sinnvoll. Auch sollte man stets als Schutz gegen bösartige „aktive Inhalte", die beispielsweise ein Ausspähen der Daten oder Manipulationen erlauben, ActiveX und JavaScript deaktivieren.

> **?** ***ActiveX***
>
> *ActiveX ist eine Programmiersprache, die von der Firma Microsoft eingeführt wurde, damit Windows-Anwendungen mit der Internet-Technologie zusammenarbeiten. WWW-Seiten können dadurch um graphische Elemente oder ausführbare Programme angereichert werden. Gefahren wie Ausforschen von Nutzern, Installieren von Viren, Überlasten des Systems oder Ausführen anderer unerwünschter Funktionen bestehen bei dieser Form „aktiver Inhalte", weil prinzipiell beliebige Datei- oder Systemmanipulationen bei Windows möglich sind.*

An der Firewall müssen für deren ordnungsgemäßen Betrieb regelmäßig bestimmte Teile des Datenverkehrs protokolliert werden. Darüber hinaus kann an der Firewall oder einem eigens dazu bestimmten Rechner auch die Kontrolle der eingehenden Daten auf schädliche Inhalte stattfinden. Solche können z. B. kleine Programme wie ActiveX-Applets sein, die beim Ansteuern einer Seite im WWW aktiviert und auf den Computer des Benutzers übertragen werden, wo sie möglicherweise ein unerkennbares Eigenleben führen. Die Kontrolle der Inhalte kann aber auch auf Viren abzielen, die sich in den an E-Mails angehängten Dateien befinden.

Die Protokollierungen und die Inhaltskontrolle sind zwar zur Aufrechterhaltung der Datensicherheit nötig. Sie sind jedoch aus datenschutzrechtlicher Sicht nicht unproblematisch, da sie das **Potential zur** umfassenden **Überwachung** der Beschäftigten bieten. Sowohl Protokollierung als auch Inhaltskontrolle bewegen sich daher auf einem schmalen Grat rechtlicher Zulässigkeit: Sie sind zwar als Maßnahme der Datensicherheit geboten, finden aber ihre Grenzen an den Vorschriften zum Schutz des informationellen Selbstbestimmungsrechts.

Der Schutz ist unterschiedlich, je nachdem, ob es sich um Datenverkehr, der dem dienstlichen Bereich zuzuordnen ist, oder um private Telekommunikation der Beschäftigten handelt. Im ersten Fall ist die Verwendung der Daten zur **Kontrolle der Arbeitsleistung** der Beschäftigten nicht völlig ausgeschlossen. Die Eingriffe in das Persönlichkeitsrecht der Beschäftigten müssen aber im Rahmen der Verhältnismäßigkeit bleiben; so wäre z. B. eine lückenlose Kontrolle der Inhalte der von einem Beschäftigten versandten E-Mails ohne Anlaß nicht zulässig. Außerdem müssen die Mitbestimmungsrechte der Mitarbeitervertretungen (Perso-

nalrat, Betriebsrat) beachtet werden. Mitbestimmungsrechte sind schon betroffen, wenn eine technische Einrichtung zur Überwachung der Mitarbeiter nur geeignet ist.

Ist den Beschäftigten die Nutzung des Internet-Anschlusses auch für die private Kommunikation erlaubt, dürfen also z. B. **private E-Mails** gesendet und empfangen und darf zu privaten Zwecken im WWW gesurft werden, so gilt insoweit das Fernmeldegeheimnis. Die entsprechenden Kommunikationsvorgänge stehen dann unter einem besonderen Schutz gegen den Zugriff des Arbeitgebers oder Dienstherren.

Jede Stelle, die eine Firewall einrichten will, muß jedenfalls schon in der Policy definieren, in welchem Umfang Protokollierungen und Inhaltskontrollen geplant sind. Für die konkrete Regelung auf Ebene des Betriebes oder der Dienststelle bietet sich dann wegen des ohnehin bestehenden Mitbestimmungsrechts der Abschluß einer **Betriebs- bzw. Dienstvereinbarung** an.

> ***? JavaScript***
>
> *JavaScript gehört ebenfalls zu den Programmiersprachen, mit denen „aktive Inhalte" für mehr Interaktivität mit dem Nutzer realisiert werden. Diese plattformunabhängige Skriptsprache wurde von der Firma Netscape entwickelt. Bei WWW-Seiten können damit Eingaben überprüft, Berechnungen durchgeführt oder Browserfunktionen angesprochen werden. Im Gegensatz zu ActiveX-Komponenten ist ein Zugriff auf Dateisysteme des Nutzerrechners nicht möglich. Vor allem durch Implementierungsfehler ist es jedoch bei einigen Browserversionen zum Ausforschen von Nutzern und zur Überlastung der Systeme gekommen.*



Wegen der Vielfalt der denkbaren Konstellationen sind hier abschließende Bewertungen nicht möglich. Einzelheiten können aber im Beratungsgespräch mit dem Landesbeauftragten für den Datenschutz oder in den entsprechenden Kursen der DATENSCHUTZAKADEMIE geklärt werden.

Was ist zu tun?
Wer sich ans Internet anschließt und personenbezogene Daten im System verarbeitet, muß diese schützen, z. B. mit Hilfe eines Firewall-Systems.

7.1.3 Gut, daß wir verschlüsselt haben !

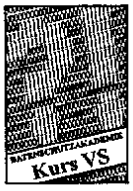
Es geht niemanden außer dem Absender und dem Empfänger etwas an, was in einer elektronischen Nachricht (E-Mail) steht. Bei der Versendung über das Netz ist ihr Inhalt jedoch offen zugänglich wie auf einer Postkarte. Diese Problematik ist vielen inzwischen bewußt. Auch die Lösung ist bekannt: E-Mails verschlüsseln!



Wie dies mit Hilfe der Software **„Pretty Good Privacy" (PGP)** (vgl. 20. TB, Tz. 7.3.2) in die Praxis umgesetzt werden kann, ist auf unserer Webseite **http://www.datenschutz.inside.tm/pgp/** beschrieben. Neben der Verschlüsselung kann der Nutzer seine Nachrichten auch digital signieren (vgl. Tz. 7.6), d. h. so versiegeln, daß sich mögliche Änderungen oder Fälschungen seiner Nachrichten vom Empfänger erkennen lassen. Ein Informationsblatt mit Informationen zum Thema „Verschlüsseln – ich?" haben wir in Kooperation mit dem Europäischen Verbraucherzentrum Kiel herausgegeben, um den Einsatz von Verschlüsselungen zu fördern. Das Faltblatt, das sich weniger an die Freaks, sondern an ganz normale Internet-Nutzer wendet, ist sowohl in den Verbraucherzentralen als auch bei uns erhältlich.

Es stehen verschiedene Versionen von PGP zur Verfügung. Universell einsetzbar ist z. B. die **Version PGP 2.6.3in**, die auch über die oben genannte Webseite abgerufen werden kann. Diese Version wurde von deutschen Programmierern überarbeitet – wer sich dafür interessiert, kann dies im offengelegten Quelltext der Software nachvollziehen – und wird bei den Zertifizierungsstellen des Individual Network e. V. eingesetzt. Im Internet gibt es auch neuere 5er- und 6er-Versionen von PGP, die aber nicht unbedingt besser sind. Denn mittlerweile wurde in diesen Versionen die Funktion eines elektronischen Brieföffners eingebaut: E-Mails, die nicht mit einem Master-Schlüssel zu dechiffrieren sind, lassen sich sogar automatisch abweisen. Was für eine Firma sinnvoll sein kann, um der Leitung einen Zugriff auf die dienstliche Post der einzelnen Mitarbeiter zu ermöglichen, kann mißbraucht werden, wenn Dritte auf diese Weise an den Inhalt von E-Mails gelangen können.

PGP ist derzeit schon ein **De-facto-Standard** für die Verschlüsselung von E-Mail im Internet. Zur Zeit wird daran gearbeitet, die PGP-Spezifikationen offiziell als „OpenPGP" zu standardisieren. Damit würden u. a. herstellerunabhängige Weiterentwicklungen von PGP unterstützt.



Mit der Herausgabe des Faltblattes und der Einrichtung unserer Serviceseite im Internet wollen wir auch ein praktisches Beispiel für den „neuen Datenschutz" geben: Datenschutz als Hilfe zum Selbstschutz. Dem Landesbeauftragten für den Datenschutz Schleswig-Holstein können übrigens PGP-verschlüsselte E-Mails zugeschickt werden.

Was ist zu tun?
Persönliche, behördliche und geschäftliche E-Mails sollten nur noch verschlüsselt verschickt werden. Wenn der Empfänger noch kein Verschlüsselungsprogramm einsetzt, sollte er auf diese Möglichkeit hingewiesen werden. Jede Verwaltung mit E-Mail-Anschluß sollte anbieten, daß die Bürgerinnen und Bürger verschlüsselt mit ihr kommunizieren können.

7.1.4 Platform for Privacy Preferences (P3P): US-Firmen zieren sich

Der Datenschutz beim Surfen im Internet soll trotz weltweit unterschiedlicher Datenschutzregelungen gewährleistet werden – und zwar mit technischer Unterstützung. P3P heißt ein Projekt, das auf eine US-amerikanische Initiative zurückgeht und das zu einem fairen Umgang der Anbieter mit den personenbezogenen Daten der Nutzer führen soll.

Im Internet gibt es viele Möglichkeiten, Daten über die Abrufer von Webseiten zu sammeln. Manchmal werden die Nutzer auch direkt nach ihren Daten gefragt, z. B. bevor ihnen Software zur Verfügung gestellt wird oder wenn Lieferanschriften oder Bankverbindungen notwendig sind. Nun ist der Datenschutz nicht überall (gleich) geregelt. Gerade die USA haben bislang auf eine Selbstregulierung der Wirtschaft statt auf gesetzliche Regelungen gesetzt. Daß immer mehr Internet-Nutzer Angst haben, daß über sie Daten gesammelt und mißbräuchlich genutzt werden, merkte auch das Standardisierungsgremium **World Wide Web Consortium** (W3C) in den USA und initiierte das Projekt P3P (Platform for Privacy Preferences).

? ***P3P***

P3P (Platform for Privacy Preferences Project) steht für einen Internet-Standard des World Wide Web Consortiums (W3C), bei dem der Nutzer eine Kontrolle über seine Daten erhält, indem er zustimmen oder untersagen kann, daß seine Daten übermittelt werden. Dafür legt er fest, welche personenbezogenen Daten er welchem Anbieter zu welchem Zweck hergeben möchte. Der Anbieter wiederum definiert, welche Daten er benötigt und wie er sie verwenden will. Nur wenn diese beiden Anforderungen von Nutzer und Anbieter im Einklang stehen, werden die Daten übermittelt.

P3P ist ein technischer Standard, mit dem Webseiten-Anbieter und Nutzer auf ihren jeweiligen Rechnersystemen **„Datenschutz-Einstellungen"** vornehmen können, die automatisch gegeneinander abgeglichen werden. Der Anbieter beschreibt, welche Nutzerdaten er zu welchen Zwecken verarbeiten will; der Nutzer legt fest, welche Daten er zu welchem Zweck herzugeben bereit ist. Damit soll der Nutzer eine Art Einwilligung in die Datenverarbeitung beim Anbieter (**„informed consent"**) geben. Da das Ganze international funktionieren soll, haben weltweit Experten an diesem Standard mitgearbeitet. Über die Europäische Union erhielten wir Gelegenheit zur Mitarbeit und zur Überprüfung der Vereinbarkeit mit dem deutschen Multimediarecht.

Wir wiesen darauf hin, daß eine rein technische Lösung für den deutschen und europäischen Rechtsbereich nicht ausreicht, da zusätzlich Kontrollmechanismen dafür vorgesehen werden müßten, daß die Anbieter sich tatsächlich an ihre eigenen Datenverarbeitungsvorgaben halten. Mit dem technischen Lösungsansatz würden sich auch nicht die Rechte der Nutzer oder die Pflichten der Anbieter erschöpfen. Zudem muß das **nationale Multimediarecht** (vgl. 20. TB, Tz. 7.1) von deutschen Anbietern beachtet werden, insbesondere

- der Grundsatz der Datensparsamkeit und die Möglichkeit für die Nutzer, Dienste anonym oder unter Pseudonym in Anspruch zu nehmen, soweit technisch möglich und zumutbar,
- die vorgegebene Form der Einwilligung des Nutzers, beispielsweise mit digitaler Signatur, und
- daß die Erbringung von Diensten nicht davon abhängig gemacht werden darf, daß der Nutzer Daten über sich preisgibt.

Dies haben wir auch in die Richtlinien für Anbieter und Programmierer einfließen lassen, damit die Standardeinstellungen in den P3P-Produkten (z. B. installiert in verschiedenen Web-Browsern) möglichst datenschutzfreundlich ausgestaltet werden.

Der P3P-Standard sollte bereits in der ersten Jahreshälfte 1998 zum Einsatz kommen. Doch haben die großen Browser-Firmen, obwohl sie an der Erstellung des Standards mitwirkten, noch keine Implementierungen in ihren Programmen vorgesehen. Auch hat der amerikanische Enthusiasmus abgenommen, nachdem sowohl die EU als auch die Fachverbände deutlich gemacht haben, daß die Selbstregulierungslösung mit technischer Unterstützung in der geplanten Form nicht ausreicht, sondern auch Mechanismen eingeführt werden müssen, um Nutzern gegebenenfalls zu ihrem Recht zu verhelfen und Verfehlungen von Anbietern zu ahnden. Zu *einer* Verbesserung haben das Projekt und die internationale Datenschutzdiskussion jedoch schon geführt: Viele Anbieter beschreiben in einer „Privacy Policy" auf ihrer Webseite, welche Daten sie wozu verarbeiten wollen.

Was ist zu tun?
Den Wünschen der Internet-Nutzer nach mehr Datenschutz muß Rechnung getragen werden. Dies kann durch technische Mechanismen unterstützt werden. In jedem Fall muß aber die tatsächliche Datenverarbeitung nicht nur in Deutschland kontrolliert werden.

7.1.5 Jugendschutz im Internet – Möglichkeiten und Grenzen

Die Schulen sollen ans Netz – vielleicht auch schon bald die Kindergärten? Das Internet ist ein Riesen-Pool mit Informationen. Nicht alle Inhalte sind jugendfrei. Leider werden auch illegale Inhalte transportiert, selbst wenn der Anteil, gemessen an den vielen nützlichen Informationen, gering ist. Die Verfolgung der Kinderpornographie im Internet ist ein wichtiges Anliegen, für das die allgemeinen gesetzlichen Vorschriften gelten.

In letzter Zeit wurde in den Medien intensiv über die Möglichkeit, per Internet **kinderpornographische Bilder** zu übertragen, berichtet. Sowohl die Verbreitung als auch der Besitz derartiger Bilder sind strafbar, d. h. jeder Abruf, jedes Speichern und jede Weitergabe, egal ob elektronisch oder auf Papier. Wir haben an der Erstellung eines **Faltblattes**, herausgegeben von den Kieler Organisationen Widerspruch e. V., dem Jugendamt und dem Präventionsbüro Petze, mitgewirkt, das Tips gibt, was man tun kann und sollte, wenn man mit solchen Inhalten in Berührung kommt.

Ein Ansatz zur Bekämpfung illegaler Inhalte besteht in der **Meldung bei Polizeidienststellen** oder über Hotlines, von denen mehrere zum Schwerpunkt Kinderpornographie im Jahr 1998 mit dem Ziel eingerichtet wurden, eine „**aufmerksame Internet-Nachbarschaft**" zu schaffen und eine vertrauensvolle Zusammenarbeit zwischen Internet-Nutzern, Providern und Polizei zu fördern: Hinweise können auch anonym eingehen, die Hinweisgeber müssen nicht mit einer Strafverfolgung rechnen. Damit soll jedoch keine Bürgerwehr aufgebaut oder zur Denunziation oder Selbstjustiz aufgerufen werden.

Die Initiative der Bundesländer „**Jugendschutz.net**" durchsucht per Programm die Webseiten im Internet anhand von Stichwörtern und Signaturen und wertet anschließend manuell die Ergebnisse – durchschnittlich 100 Treffer täglich – durch in diesem Bereich erfahrene Personen aus. Die Anbieter von jugendgefährdenden Inhalten mit Sitz in Deutschland, die für Minderjährige zugänglich sind, werden von der Initiative aufgefordert, die Angebote herauszunehmen oder gegebenenfalls wirksame Zugriffsbeschränkungen vorzusehen. Falls dies nicht geschieht, droht eine Weitergabe an die Ermittlungsbehörden. Bislang war dies jedoch nicht nötig.

Im Dezember 1998 lud das **Bundeskriminalamt** Provider und Vertreter von Ministerien, Ermittlungsbehörden und Datenschutzbeauftragten zu einem Workshop „Bekämpfung der Kriminalität im Internet" ein. Nach den Multimediagesetzen haben die Provider keine Verpflichtung, eine umfassende Überprüfung der Internet-Inhalte vorzunehmen. Dies wäre wegen der riesigen Menge und des erforderlichen juristischen Spezialwissens in vielen Fällen auch nicht möglich. Allerdings müssen sie auf Hinweise reagieren und Inhalte nach Möglichkeit entfernen oder die Meldungen an Ermittlungsbehörden weitergeben. Die Provider stellten klar, daß sie durchaus die Polizei unterstützen und Daten in der benötigten Weise herausgeben würden, vorausgesetzt, es liegt der gesetzlich vorgesehene

richterliche Beschluß bzw. – bei Gefahr im Verzuge – eine staatsanwaltschaftliche Entscheidung vor.

Der Polizei reicht das nicht. Gerne würden die Ermittler auch ohne diese Voraussetzungen auf solche Daten zugreifen und die Provider zu einer Art **„Hilfssheriffs"** im Internet verpflichten. Zur rechtlichen Begründung wird auf eine Vorschrift aus dem Telekommunikationsdatenschutzrecht zurückgegriffen, nach der bei „Störung und Mißbrauch von Telekommunikationseinrichtungen" bestimmte Datenerhebungen und -verarbeitungen zulässig sind. Die betreffende Norm, § 7 Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV), kann jedoch keine Rechtsgrundlage für Inhaltskontrollen sein, die in das Fernmeldegeheimnis eingreifen, da sie sich wie das gesamte Telekommunikationsrecht nur auf die Ebene der Übertragungsleitungen, nicht auf die Inhalte bezieht. Wir hoffen, daß die Aspekte des grundrechtlichen Fernmeldegeheimnisses bei der Arbeitsgruppe Berücksichtigung finden, in der der Informationsaustausch fortgesetzt werden soll.

Wenn es nicht um illegale Inhalte, sondern darum geht, zu Hause oder in der Schule keine jugendgefährdenden Webseiten anzuzeigen, können sich Eltern und Lehrer von **Filtersoftware** unterstützen lassen. Solche Programme bieten die Möglichkeit, den Abruf von als ungeeignet eingestuften Inhalten zu versperren und die Online-Zeit zu begrenzen. Häufig werden die Inhalte über die Adresse im Internet identifiziert: Statt Negativlisten für zu sperrende Webseiten lassen sich auch Positivlisten für ausgewählte kinderfreundliche Angebote einstellen. Dies bietet sich insbesondere für jüngere Altersgruppen an. Andere Methoden basieren auf vorgegebenen Suchwörtern oder anderen automatisiert auswertbaren Kriterien. Differenzierter kann man beim Abgleich mit an die Webseite angehängten Bewertungen arbeiten.

Leider hat sich bei all diesen Verfahren gezeigt, daß sie auch mißbraucht werden können, um unliebsame Inhalte, z. B. kritische Stimmen, zu unterdrücken, und daß ungewollt auch unbedenkliche Inhalte ausgefiltert werden. Bedingung für einen sinnvollen Einsatz dieser Programme ohne einen Anstrich von **„Zensur"** ist eine transparente und konfigurierbare Arbeitsweise unter der Kontrolle des Nutzers. Die Programme stellen keine perfekte Lösung dar, denn es gibt immer Möglichkeiten, die Sperrungen zu umgehen.

Jugendschutz bedeutet auch Schutz der personenbezogenen Daten der Kinder, die im Internet Spuren hinterlassen. Gute technische Lösungen sind durch Mix-Systeme (vgl. Tz. 7.1.1) erreichbar; auch P3P (vgl. Tz. 7.1.4) sieht spezielle Kindereinstellungen vor, die vor der Übermittlung der Nutzungsdaten schützen sollen.

Was ist zu tun?

Die Diskussion über illegale oder jugendgefährdende Inhalte im Internet sollte von allen Beteiligten sachlich geführt werden. Maßnahmen gegen den Transport von kinderpornographischen Inhalten im Internet müssen sich am Maßstab des grundrechtlich geschützten Fernmeldegeheimnisses messen lassen.

7.2 Biometrie datenschutzgerecht gestalten

Legitimation per Daumenabdruck – was bis jetzt vor allem aus Hochsicherheitstrakten und James-Bond-Filmen bekannt ist, soll immer mehr Einzug in das alltägliche Leben halten: die Biometrie. Nun kommt es darauf an, daß diese Technologie für den Datenschutz der Menschen und nicht für deren Überwachung eingesetzt wird.

Um sich gegenüber einem Bankautomaten oder Computersystem zu identifizieren, werden heutzutage hauptsächlich Mechanismen wie Paßwort und PIN („Wissen") oder Chipkarten („Besitz") verwendet. Hier besteht des Problem des „Vergessens" bzw. des Verlusts. **Biometrische Verfahren**, die auf Charakteristika des individuellen Menschen („Sein") beruhen, haben demgegenüber den Vorteil, daß sie nicht einfach gestohlen oder ausgespäht werden können und häufig komfortabler zu bedienen sind. Damit können sie zu einer besseren Datensicherheit beitragen. Typische Einsatzbereiche liegen in der Zugangs- oder Zugriffskontrolle. Doch auch bei der Abgabe von Willenserklärungen, z. B. im Zusammenhang mit der digitalen Signatur (vgl. Tz. 7.6), können biometrische Verfahren zur Freischaltung eines privaten Schlüssels dienen. Für Verfahren nach dem Signaturgesetz ist zur Zeit geregelt, daß biometrische Merkmale zusätzlich zu einer Identifikation des Inhabers durch Besitz und Wissen nutzbar sind (§ 16 Abs. 2 SigV).

> **? *Biometrische Verfahren***
>
> *Mit Biometrie (abgeleitet von Leben (Bio) und Lehre des Messens (Metrie)) bezeichnet man Methoden, die physiologische und Verhaltensmerkmale von Personen auswerten. Dazu gehören der Fingerabdruck, die Stimme, das Aussehen, die Unterschrift oder die Anschlagdynamik auf einer Tastatur. Diese Verfahren lassen sich zur Identifikation von Personen einsetzen.*

Damit ein biometrisches System eine Person erkennen kann, müssen die Informationen, mit denen später ein Abgleich erfolgen soll, in einer **Referenzdatenbank** gespeichert werden. Dazu werden die ausgewählten Merkmale der Person von biometrischen Sensoren erfaßt, digitalisiert und nach bestimmten Regeln zu komprimierten Referenzdaten umgewandelt. Bei einer späteren Identifizierung vergleicht das System die Informationen, die aktuell von den Sensoren gemeldet werden, mit den abgespeicherten Datensätzen und meldet gegebenenfalls eine Übereinstimmung. Hierbei lassen sich Fehler nicht vollständig ausschließen: Es können Nutzer fälsch-

> **? *Biometrische Fehlerraten***
>
> *Man unterscheidet zwei Fehlerraten bei biometrischen Systemen: Die False Rejection Rate (FRR) drückt aus, wie hoch der Anteil der fälschlich vom System zurückgewiesenen Nutzer ist; die False Acception Rate (FAR) beschreibt den Anteil der fälschlich zugelassenen Personen. Vielfach verwendet man zur Konfiguration des biometrischen Systems den Wert, bei dem beide Raten gleichermaßen möglichst klein sind: die Equal Error Rate (EER). Je nach gefordertem Sicherheitsniveau kann man die Fehlerratenparameter ändern.*

lich zugelassen wie auch fälschlich zurückgewiesen werden. Diese beiden Fehlerraten sind voneinander abhängig, d. h., wenn die eine steigt, sinkt die andere. Daher muß man für ein hohes Sicherheitsniveau das System so konfigurieren, daß möglichst keine Person fälschlich akzeptiert wird, man jedoch berechtigten Nutzern gegebenenfalls mehrere Versuche zumutet, bis sie erkannt werden.

Biometrische Daten sind nicht nur personenbezogen, sondern meist auf Dauer personengebunden und daher besonders sensibel. Biometrische Sensoren können unter Umständen mehr Informationen aufnehmen und analysieren als für die Identifikation der Person benötigt werden (z. B. bestimmte Krankheiten oder die momentane Stimmung der Person). Auch **Überwachungstechnologien** profitieren von der Biometrie. So gibt es Videoüberwachungssysteme, die es ermöglichen, einzelne Personen anhand ihrer Gesichter selbst in großen Menschenmengen zu erkennen und auf ihrem Weg zu verfolgen. In China werden mit derartigen Methoden noch heute Teilnehmer an den Demonstrationen auf dem Platz des Himmlischen Friedens identifiziert, anschließend verurteilt und jahrelang in Arbeitslager gesteckt. .

Die gespeicherten Referenzdaten der Personen können ausgewertet werden. Dies ist besonders bedenklich, wenn sie unmittelbar die Identität des Betroffenen offenbaren. Dadurch könnte z. B. das polizeiliche System der **erkennungsdienstlichen Sammlungen** geradezu revolutioniert werden. Statt entsprechend den rechtsstaatlichen Vorschriften eigene Sammlungen aufzubauen, könnte die Polizei auf die biometrischen Datenbanken in privater Hand zurückgreifen.

Von der Ausgestaltung der Verfahren hängt ab, ob sich die Biometrie zu einer datenschutzfeindlichen oder datenschutzfreundlichen Technologie entwickelt. Zu den **Datenschutzanforderungen** gehört beispielsweise, daß

- das Verfahren eine aktive Mitwirkung des Nutzers benötigt, damit keine Daten unerkannt erhoben werden,
- die gespeicherten Daten unter der Kontrolle des Betroffenen stehen und z. B. in seinem Verfügungsbereich auf einer Chipkarte o. ä. gespeichert sind und
- die Daten verschlüsselt im System so abgelegt sind, daß für einen Zugriff im Klartext eine aktive Freischaltung durch den Nutzer erfolgen muß.

Diese Ideen bringen wir in ein Pilotprojekt zum **Electronic Banking** ein, das von Biometrie-Herstellern des TeleTrusT e. V. unter Mitwirkung von Verbraucherschutz und Datenschutz ab 1999 durchgeführt werden soll. Hier sollen verschiedene biometrische Verfahren für eine Zugangskontrolle im Bankenbereich, an Geldautomaten und beim Homebanking erprobt und geprüft werden. Schon im Vorfeld wird die Bereitschaft der Hersteller deutlich, die Anforderungen des Daten- und Verbraucherschutzes möglichst gut in ihren Systemen umzusetzen. Wir haben die Einladung angenommen, durch die Begleitung des Projektes konstruktiv zur datenschutzgerechten Technikgestaltung bei biometrischen Verfahren beizutragen.

Was ist zu tun?
Gerade bei so sensiblen Technologien wie der Biometrie sollten Hersteller und Anwender Datenschutzexperten von Anfang an einbinden, um die Verfahren nicht nur (datenschutz)rechtlich einwandfrei zu realisieren, sondern mit ihnen sogar einen besseren Datenschutz erreichen zu können. Nur so läßt sich eine Akzeptanz bei den Nutzern erreichen.

7.3 Data-Warehouse und Data-Mining heben Zweckbindung auf

Neue Werbebotschaften der Softwareindustrie zum *Data-Warehouse* und zu *Data-Mining* kündigen eine grundlegende Veränderung in der Datenverarbeitung an. Es geht um die Entdeckung, daß in den umfangreich gespeicherten Daten weitaus mehr Erkenntnisse stecken können als auf den ersten Blick erkennbar ist. Der Zweckbindungsgrundsatz setzt Data-Warehouse und Data-Mining Grenzen.

> **? Data-Warehouse**
> *Ein Data-Warehouse faßt alle in einer Organisation vorhandenen Daten in einer einheitlichen Datenbank zusammen, so daß sämtliche Informationen für beliebige Zwecke verknüpfbar zur Verfügung stehen.*

Um das gesamte Wissenspotential zu erschließen, sollen die in Unternehmen oder sonstigen Organisationen verstreut gespeicherten Datenbestände zusammengeführt werden, so daß alle Informationen wie in einem Warenlager einheitlich geordnet zur Verfügung stehen. Aus diesem **Data-Warehouse** sollen dann sämtliche Informationen für jederzeitige und beliebige Auswertungen genutzt werden können. Die Daten stehen also nicht mehr nur im Zusammenhang des Zwecks, zu dem sie ursprünglich erhoben wurden, sondern sie dienen darüber hinaus allen weiteren Informationswünschen, die gerade bestehen oder zukünftig bestehen könnten. Dabei wird die Schutzfunktion der begrenzten Nutzung von Informationen, die Zweckbindung, schlicht aufgehoben.

> **? *Data-Mining***
> *Unter Data-Mining versteht man die automatisierte Suche nach bisher nicht bekannten Zusammenhängen in großen Datenbeständen. Als Grundlage für die Suche dient das Data-Warehouse.*

Aus den zusammengeführten Daten lassen sich Informationen gewinnen, die vorher nicht erkennbar waren. Beim **Data-Mining** (engl. Daten-Bergbau) wird durch den Datenberg des Warehouse gegraben, um wissenswerte Zusammenhänge aufzuspüren. Grundidee des Data-Mining ist es, den Computer selbständig nach unbekannten oder verborgenen Mustern oder Trends suchen zu lassen, um auf diese Weise zu neuen Erkenntnissen zu gelangen, die dem Eigentümer des Warehouse nutzen könnten.

Wissen ist Macht – zumindest kann es einen geldwerten Vorteil bedeuten. Eine Handelskette, die – aus Datenbeständen abgeleitet – weiß, daß Väter gern Bier

mitnehmen, wenn sie im Supermarkt Windeln für die Kleinen kaufen, kann ihr Sortiment strategisch plazieren und den Absatz steigern. Mag dieses Beispiel auch ein vielzitierter **EDV-Mythos** sein – mit der Harmlosigkeit solchen Wissens über Menschen ist es jedenfalls schnell vorbei, wenn der Kunde als identifizierbares Wesen unter die Lupe genommen und bewertet wird. Die Analyse seines Verhaltens führt zu Erkenntnissen, welchen Nutzen er dem Unternehmen bisher gebracht hat bzw. welcher für die Zukunft zu erwarten ist.

Wenn die automatisierte Auswertung der über ihn angehäuften Fakten zu seinen Ungunsten ausfällt, kann er von einem auf den anderen Tag in „Ungnade" fallen, weil man sich keinen ausreichenden Gewinn mehr von ihm verspricht. Wie sein „**Kundenwert**" im einzelnen bestimmt wird, erfährt er nicht. Vielfach wird er nicht einmal bemerken, daß sich das Verhalten eines Unternehmens auf gespeicherte Daten gründet, die mit bestimmten Annahmen verbunden als Rechenergebnis vom Computer geliefert wurden.

Das kundenorientierte Sammeln von Daten im Data-Warehouse bedeutet nichts anderes als das Anlegen von **Dossiers über Menschen**. Nun liegt es Unternehmen fern, ihre Kunden umfassend bespitzeln und somit beherrschen zu wollen. Ausschlaggebend ist zumeist nur die Hoffnung auf ein verbessertes Geschäftsergebnis. Dennoch ist das Horten von vermeintlichem oder zutreffendem Wissen über den unmittelbaren Geschäftszweck hinaus in einem übergreifenden Datenbestand nicht unproblematisch. In Verbindung mit personenbezogenen Daten bedeutet das Konzept des Data-Warehouse und des Data-Mining geradezu die **Umkehrung des Datenschutzgedankens**. Wo Informationen aus unterschiedlichsten Sinnzusammenhängen entnommen und von ihren ursprünglichen Zwecken entfernt werden, um ein übergreifendes und für beliebige Ziele verwendbares Datenlagerhaus zu schaffen, sind Menschen, um deren Daten es geht, nicht mehr in der Lage, zu überblicken, woher die Einzelinformationen stammen. Wird das Datenlagerhaus mit den Methoden des Data-Mining durchforstet, entsteht zusätzliches „Wissen", das vorher aus den gesammelten Einzelinformationen nicht zu ersehen war. Dies können Erkenntnisse sein, die sogar den betroffenen Menschen überraschen würden, sofern er denn davon erführe.

Nach dem Datenschutzrecht sind Data-Warehouse und Data-Mining mit personenbezogenen Daten enge Grenzen gesetzt, weil Daten nur im Rahmen ihrer ursprünglichen **Zweckbestimmung** verarbeitet werden dürfen. Auch eine Einverständniserklärung des Betroffenen scheidet aus, weil der Verwendungszweck der Daten des Warehouse eben nicht feststeht, sondern sich je nach Bedarf verändert. Wirtschaftsunternehmen sollten sich über die Gesetzeslage also rechtzeitig informieren, bevor sie mit großem Aufwand ein Data-Warehouse aufbauen.

Was derzeit in der Privatwirtschaft diskutiert wird, findet über kurz oder lang auch in der **öffentlichen Verwaltung** Nachahmung. Im Hinblick auf personenbezogene Daten wird zweifellos auch hier das Wunschbild nach übergreifenden Datenbeständen und -recherchen entstehen. Was bisher vor allem im Bereich der Sozialverwaltung unter dem Stichwort des Datenabgleichs diskutiert wurde, könnte zukünftig über den Begriff des Data-Warehouse als neuartige Problemlösung für

die Verwaltung entdeckt werden: die Zusammenführung unterschiedlichster bereits vorhandener Daten zur Aufdeckung bisher übersehener (sozialstaatlicher) Einsparmöglichkeiten mittels Data-Mining. Die Neukonzeption des polizeilichen Datenverarbeitungssystems unter der Bezeichnung **INPOL-neu** ist ein Schritt in diese Richtung (vgl. Tz. 4.2.2).

Was ist zu tun?
Wer ein Data-Warehouse oder vergleichbare Lösungen in der Datenverarbeitung einsetzen will, muß zunächst die Vereinbarkeit mit den Zweckbindungsvorschriften prüfen. Für die öffentliche Verwaltung scheiden derartige Konzepte schon deswegen regelmäßig aus.

7.4 Krypto aktuell

Den jährlichen Bericht über die Entwicklung möglicher Kryptoregulierungen kann man schon als ständige Rubrik betrachten. Das Thema ist nach wie vor aktuell und noch lange nicht vom Tisch. Es hat sich geradezu ein Wettlauf zwischen den Verfechtern des Schutzes der Privatsphäre durch Verschlüsselung und Angriffen auf die Verschlüsselung ergeben. Hier also die Krypto-News von 1998.

Anfang des Jahres zeigte die amerikanische Datenschutzorganisation **Electronic Frontier Foundation (EFF)**, daß man in 2 ½ Tagen einen 56-Bit-Schlüssel des Data Encryptionstandards (DES) knacken kann. Diese Verschlüsselungsmethode haben die deutschen Banken bis Ende 1997 eingesetzt. Die EFF-Mitglieder bauten für den „**Knackwettbewerb**" eine Maschine, die aus 1 800 parallel arbeitenden Spezialchips names „Deep Crack" besteht. Die Kosten für diesen Prototyp betrugen knapp 250 000 US-$; bei der Produktion von mehreren derartigen Maschinen würde der Preis deutlich sinken. Baupläne für den Nachbau des DES-Cracker sind in Buchform erschienen. Mittlerweile liegt der Knack-Weltrekord für DES bei nur noch 22 Stunden. Bei kürzeren Schlüsseln, z. B. mit einer Länge von 40 Bit, wie sie Anfang 1998 in der Regel in der Exportsoftware aus den USA erlaubt war, braucht die Maschine nur etwa 6 Sekunden.

Kurze Zeit später führte der Mathematiker Ronald L. Rivest ein Verfahren vor, das zwar auf jede Form der Verschlüsselung verzichtet, aber dennoch Nachrichten gegen unberechtigte Mitleser schützen kann: „**Chaffing and Winnowing**" (deutsch etwa: „die Spreu vom Weizen trennen"). Dabei wird die zu übermittelnde Botschaft in kleine Blöcke (man stelle sich beispielsweise vor, in der Länge von einem Buchstaben) unterteilt, die gemischt mit vielen anderen bedeutungslosen Blöcken transportiert werden. Nur Absender und Empfänger wissen, welche Blöcke zur eigentlichen Nachricht gehören, und können die Botschaft wieder zusammensetzen. Das Zumischen von sinnlosen Blöcken kann auch durch einen Dritten automatisiert erfolgen. Man kann diese Methode als eine Form der Steganographie auffassen, die sich durch eine Kryptoregulierung nicht verhindern läßt (vgl. 20. TB, Tz. 7.3.1; 19. TB, Tz. 7.6).

Vor diesem Hintergrund haben die **USA** mehrfach die **Exportbestimmungen** für **Kryptoprodukte** geändert. Dennoch besteht weiterhin die Pflicht, daß in fast allen Bereichen wirksame Kryptographie nur ausgeführt werden darf, wenn es möglich bleibt, bei Bedarf die verwendeten Schlüssel zu rekonstruieren (Key Recovery). Immer wieder wurden außerdem Versuche der Vereinigten Staaten bekannt, diese Politik auch in anderen Ländern, z. B. in Europa, durchzusetzen. Die Auswirkungen des **Wassenaar-Abkommens**, die kurz vor Weihnachten beschlossen wurden, sind noch nicht völlig klar. Aus dem Bundesausfuhramt verlautete immerhin schon, daß mindestens Software für den Massenmarkt wie „Pretty Good Privacy (PGP)" (vgl. Tz. 7.1.3) nicht unter eine Exportrestriktion falle.

> ***? Wassenaar-Abkommen***
>
> *Das Ende des Kalten Krieges beendete auch das COCOM-Regime, mit dem die westlichen Industriestaaten den Export militärisch wie zivil (Dual-Use) nutzbarer Güter koordinierten und in dem seit Jahren auch der Export von Computertechnik reguliert wird. Ersetzt wurde diese Koordination durch das Wassenaar-Abkommen, dem heute auch Rußland und andere ehemalige Ostblockstaaten angehören. In deutsches Recht umgesetzt werden die Vereinbarungen weiterhin in den Anlagen zum Außenwirtschaftsgesetz.*

Kompromittierende Strahlung ist heute zu einem Sicherheitsproblem auch ziviler Computernutzung besonders für Unternehmen geworden. In einigen Ländern, u. a. in den USA, ist geplant, einen „Großen Computerlauschangriff" zu legalisieren, bei dem kompromittierende Abstrahlung ausgewertet und Trojanische Pferde eingesetzt werden. Auch hier zeigt sich, daß der Schutz von Daten einen zunehmenden technischen Aufwand erfordert.

> ***? Kompromittierende Strahlung***
>
> *Nach dem zweiten Weltkrieg entdeckte die britische Spionageabwehr, daß elektrische Schreibmaschinen Signale abgeben, durch die der getippte Text beim Anzapfen der Stromleitung lesbar wird. Deutlicher noch sind die Signale, die normale Bildschirmgeräte abgeben und die per Funk in Hunderten von Metern Distanz lesbar sind. Das Militär nutzte seit den 70er Jahren kompromittierende Strahlung elektronischen Geräts aller Art als Mittel der Nachrichtenbeschaffung. Verbreitete Kenntnis und geringe Kosten machen kompromittierende Strahlung heute zu einem Sicherheitsproblem auch ziviler Computernutzung besonders für Unternehmen.*

Von der neuen Bundesregierung gibt es noch keine eindeutigen Aussagen, zu einer möglichen Kryptoregulierung. Wir fördern weiterhin den Einsatz von Verschlüsselungsprogrammen und beraten auch laufend Bürger und Verwaltung. Im Entwurf des neuen Landesdatenschutzgesetzes haben wir für bestimmte Fälle eine Verschlüsselungspflicht vorgesehen.



Was ist zu tun?

Kryptographie muß frei bleiben, damit jeder die eigenen Daten wirksam schützen kann. Die Landesregierung sollte dies deutlich unterstützen und etwaigen Plänen zur Einschränkung der Kryptographie entgegentreten.

7.5 Auf dem Weg zum praktischen Einsatz der digitalen Signatur

Der praktische Einsatz der digitalen Signatur bedarf umfangreicher Vorbereitungen. Mit digitalen Signaturen ist in größerem Umfang ab 1999 zu rechnen.

Im 19. Tätigkeitsbericht (Tz. 7.7) und im 20. Tätigkeitsbericht (Tz. 7.2) hatten wir über die digitale Signatur, ihre möglichen Anwendungsbereiche und die im Jahr 1997 neu geschaffenen Rechtsvorschriften zu ihrem Einsatz berichtet. Seit dem Frühjahr 1998 wartet die Fachwelt darauf, daß erste Verfahren der digitalen Signatur nach dem Signaturgesetz in der Praxis angeboten werden. Allerdings erwiesen sich gerade die hohen **Sicherheitsanforderungen**, deren Einhaltung das Vertrauen in das Verfahren gewährleisten soll, als Bremse bei der schnellen Markteinführung. Selbst für große Anbieter war es nicht einfach, die geforderten Sicherheitsstandards in kurzer Zeit umzusetzen.

Um die vom Signaturgesetz vorgeschriebene **zweistufige Infrastruktur** der **Zertifizierungsstellen** in die Praxis umzusetzen, war zunächst die technische Einrichtung des Trust-Centers der Regulierungsbehörde für Telekommunikation und Post (RegTP) als Wurzelinstanz erforderlich. Diese Arbeit wurde von der auf Fragen der Kommunikationssicherheit spezialisierten Telekom-Tochter Telesec ausgeführt. Ende September 1998 konnte das fertige Trust-Center an die Regulierungsbehörde übergeben werden.

Inzwischen liegen bereits mehrere Anträge auf Zulassung als Zertifizierungsstelle nach dem Signaturgesetz bei der RegTP vor. Als erstes Unternehmen wird die Telekom ab Anfang 1999 die Ausgabe von Signaturzertifikaten anbieten. In den T-Punkt-Läden ist für 50 DM eine Signatur-Chipkarte mit einem Schlüsselpaar zu erwerben; weitere 100 DM werden als jährliche Gebühr für die Trust-Center-Dienstleistungen fällig. Das erforderliche Kartenlesegerät zusammen mit weiteren Sicherheitskomponenten kostet 300 DM. Es ist damit zu rechnen, daß bald weitere Genehmigungen erteilt und Zertifikate für Zertifizierungsstellen ausgegeben werden. Dies führt dann wohl zu einer für Endverbraucher akzeptablen Preissenkung. Erst dann werden die Bürger von der im Signaturgesetz vorgesehenen datenschutzfreundlichen Möglichkeit Gebrauch machen, im elektronischen Geschäftsleben auch unter Pseudonymen und mit mehreren Signaturschlüsselzertifkaten aufzutreten.



Weitere Informationen zu diesen Themen sind zu finden unter:



www.dtag.de/angebot/telesec/vertrau/digitale/index.htm
www.dtag.de/angebot/telesec/produkte/services/trust/right.htm
www.bsi.de/aufgaben/projekte/pbdigsig/index.htm
www.trustcenter.de/html/Infos/Law/405.htm
www.iid.de/iukdg/wissensforum/boerse.html

und unter der Textziffer 8.

7.6 Erstmalig Datenschutzanforderungen in den Common Criteria

Nachdem der Begriff „datenschutzfreundliche Technologien" (Privacy-Enhancing Technologies, PET) inzwischen zu einem Qualitätsmerkmal geworden ist, hat der Datenschutz mittlerweile auch Eingang in die neuen Standards zur Sicherheitszertifizierung gefunden.

„Common Criteria for Information Technology Security Evaluation 2.0" heißt der neueste Sicherheitsstandard, der im Mai 1998 fertiggestellt wurde. Er soll in Kürze zum internationalen Standard (ISO) für die Sicherheitszertifizierung von IT-Produkten und -Systemen werden. Erstmals sind darin Anforderungen zum Schutz der Privatsphäre der Nutzer formuliert. Die Rubrik „Privacy" enthält die Grundsätze zur Datensparsamkeit, Anonymität, Pseudonymität, Unverkettbarkeit und Unbeobachtbarkeit und geht damit deutlich über die bisherigen Sicherheitsziele hinaus, die sich hauptsächlich an den Interessen des Systembetreibers orientierten. Mit den Common Criteria wird eine Vergleichbarkeit der Bewertung verschiedener datenschutzfreundlicher Technologien möglich.

> **?** ***IT-Sicherheitszertifizierung***
>
> *bedeutet die Abgabe einer formalen Erklärung, die die Ergebnisse einer Prüfung (Evaluation) und die ordnungsgemäße Anwendung der benutzten Evaluationskriterien durch ein herstellerunabhängiges Prüflabor bestätigt. Damit soll zum Ausdruck gebracht werden, daß das Produkt oder das System bestimmten Sicherheitsanforderungen genügt.*

Die Erfüllung von abstrakten IT-Sicherheitskriterien allein garantiert jedoch noch keine sicheren Systeme – ebensowenig wie ein Gütesiegel dies kann. Immer ist die Einbindung in das gesamte automatisierte Verfahren und die organisatorischen Gegebenheiten zu berücksichtigen. Diese müssen ständig dem technologischen Fortschritt angepaßt werden. Zusammen mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder haben wir einen externen Experten damit beauftragt, uns über aktuelle Entwicklungen im Bereich der Zertifizierungsstandardisierung auf dem laufenden zu halten und die Interessen des Datenschutzes in den Normungsgremien in enger Abstimmung mit uns zu vertreten.

Was ist zu tun?

Inzwischen werden die ersten Zertifzierungen nach den Common Criteria vorgenommen. Inwieweit von den betroffenen Produkten die Privacy-Kriterien erfüllt werden, kann in diesen Fällen gut überprüft werden.

7.7 Umfangreiche Abhörbestimmungen in Vorbereitung

Auf Betreiben der Sicherheitsbehörden verfolgte die alte Bundesregierung das Ziel, die Telekommunikation lückenlos überwachbar zu machen. Die aktuellen Regelungsvorhaben legen allerdings die Fragwürdigkeit dieses Ansatzes offen.

Mit dem **Telekommunikationsgesetz** (TKG) wurde 1996 der letzte Schritt zur Liberalisierung des Telekommunikationsmarktes unternommen. Zugleich wurden die Regelungen zum Fernmeldegeheimnis und zum Datenschutz in diesem Bereich an die neue Lage angepaßt, weil die Telekommunikationsdienste nicht mehr eine staatliche Stelle erbringt, sondern private Unternehmen. Allerdings gab das TKG den Sicherheitsbehörden auch neue Befugnisse zum Zugriff auf die Daten über die Kundinnen und Kunden von Telekommunikationsunternehmen (vgl. 19. TB, Tz. 7.3.1). Die Pflicht zur Mitwirkung bei Überwachungsmaßnahmen traf bis dahin allerdings nur die Unternehmen, die Telekommunikationsdienste für die Öffentlichkeit anboten.

Mit dem Anfang 1998 in Kraft getretenen **Begleitgesetz zum Telekommunikationsgesetz** wurden die Mitwirkungspflichten auch auf die „geschäftsmäßigen Erbringer von Telekommunikationsdiensten" ausgedehnt. Erfaßt waren damit sämtliche Telekommunikationsanlagen (neben Telefon- auch Computernetze), deren Betreiber Dritten entgeltlich oder unentgeltlich die Benutzung erlauben oder die für unternehmensinterne Zwecke genutzt werden (vgl. 20. TB, Tz. 7.4). Damit besteht z. B. die Pflicht für Krankenhaus- und Hotelbetreiber, die ihren Patienten bzw. Gästen ein Telefon zur Verfügung stellen, die Überwachung dieser Einrichtungen zu ermöglichen und dabei mitzuwirken. Das gleiche gilt für Computernetze. Der Nachweis, daß ein Telekommunikationssystem überwacht werden kann, ist eine der gesetzlichen Voraussetzungen für dessen Betriebszulassung. Aufgrund dieser Vorschriften wäre es möglich, Telefonnebenstellenanlagen, die diesen Anforderungen noch nicht genügen, stillzulegen.

Diese umfangreichen gesetzlichen Verpflichtungen zur Mitwirkung tragen dazu bei, daß in Deutschland im internationalen Vergleich besonders viele Telekommunikationsvorgänge überwacht werden. Dennoch kam es anläßlich des Inkrafttretens des TKG nicht zu größerem Protest der betroffenen Kreise; diesen war nämlich in Aussicht gestellt worden, daß die Verpflichtungen in der nach dem TKG zu erlassenden **Telekommunikationsüberwachungs-Verordnung (TKÜV)** zumindest teilweise wieder zurückgenommen würden.

Dies war allerdings bislang nicht der Fall. Die vorgelegten Entwürfe hätten vielmehr dazu geführt, daß beispielsweise eine einzige E-Mail-Nachricht an eine überwachte Person nicht weniger als dreimal an die überwachende Behörde zu übermitteln gewesen wäre:

- Das Eintreffen der E-Mail beim Internet-Provider hätte zur ersten Übermittlung geführt, weil der Provider alle Daten, die in Zwischenspeichern abgelegt werden, unverzüglich an die überwachende Behörde zu liefern hätte.
- Der Anruf der überwachten Person per Telefonleitung bei ihrem Internet-Provider würde die Überwachung dieses Datenverkehrs auslösen. Dabei würde die E-Mail vom Telekommunikationsunternehmen ein zweites Mal an die überwachende Behörde geliefert.
- Der Internet-Provider schließlich wäre zur Übermittlung aller Datenpakete von der überwachten Person bzw. an diese verpflichtet, sobald diese Verbindung mit dem Provider aufnimmt. Gleichzeitig mit den vom Telekommunikationsunternehmen übermittelten Daten der überwachten Telefonleitung würde die überwachende Behörde auf getrenntem Wege dieselben transportierten Datenpakete vom Internet-Provider erhalten.

Bürgerinnen und Bürger müßten umfangreiche Einschränkungen des grundrechtlich geschützten Fernmeldegeheimnisses befürchten, ohne daß dies durch irgendeinen Sicherheitsvorteil aufgewogen würde. Für die Sicherheitsbehörden würden durch die **Mehrfachüberwachung** desselben Kommunikationsvorgangs die gleichen Daten mehrfach anfallen, ohne daß daraus ein Vorteil für die polizeiliche Arbeit folgen könnte. Die unnötige Belastung der Sicherheitsbehörden durch überflüssige Auswertung von doppelt und dreifach erlangtem Material würde vielmehr Arbeitskraft binden, die an anderer Stelle sinnvoller eingesetzt werden kann.

Bei den verpflichteten Unternehmen entstünden erhebliche **Kosten**, die in ihrer Gesamtheit nach ersten Berechnungen die Schäden um ein Mehrfaches übersteigen, die durch die organisierte Kriminalität entstehen, mit deren Bekämpfung die Gesetze begründet wurden. Viele kleine Telekommunikations- und Internet-Dienstleistungsunternehmen ohne eigene Infrastruktur würden durch die mit den Überwachungsauflagen verbundenen Kosten in ihrer Existenz bedroht. Die Kosten des Grundrechtseingriffs stehen hier in keinem Verhältnis zum Nutzen. Die einzig richtige Konsequenz kann nur die substantielle Verkleinerung des Kreises von Mitwirkungspflichtigen sein. Das TKG sollte dahin geändert werden, daß nur noch die Unternehmen, die Inhaber von Lizenzen sind, zur Mitwirkung bei der Überwachung verpflichtet sind.

Nach Presseveröffentlichungen zum TKÜV-Entwurf führten **Proteste** von Verbänden und Datenschützern dazu, daß das zuständige Bundeswirtschaftsministerium den Verordnungsentwurf und die Technische Richtlinie Internet zurückzog, bevor eine dazu geplante Anhörung stattfand. Die TKÜV steht in diesem Jahr erneut zur Beratung an.

7.8 Von der Europäischen Union zur Europäischen Überwachungsunion?

Ende 1998 schien es, als würden die extremen deutschen Vorstellungen zur Überwachung der Telekommunikation auch auf europäischer Ebene auf Akzeptanz stoßen. Im September beriet der EU-Ministerrat darüber, die Regelungen zur Überwachung der Telekommunikation EU-weit einheitlich an die Bedingungen im Internet und in globalen Satellitenkommunikationssystemen anzupassen.

Ein Anlaß war der Startschuß für das **Satellitenkommunikationssystem IRIDIUM**, über das Kunden überall auf der Welt mit einem Handy-ähnlichen Gerät kommunizieren können. Der globale Charakter des Systems bedingt, daß nicht mehr in jedem Staat überwachbare Satellitenbodenstationen existieren. Mit der sogenannten **ENFOPOL-Entschließung** sollten Verfahren für solche Länder etabliert werden, die rechtmäßige Überwachungsersuchen nur in Kooperation mit Staaten abwickeln können, in denen solche Basisstationen vorhanden sind.

Zugleich wurden Vorgaben für die **Überwachung des Internet** formuliert. Darin ist beispielsweise vorgesehen, auch das Paßwort und die Bankverbindung des Überwachten zu übermitteln. Sie gehen sogar über das deutsche Recht hinaus, weil ausdrücklich auch die mit **Prepaid-Karten** abgewickelte **Telekommunikation** in die Überwachung einbezogen werden soll. In der Konsequenz würde das bedeuten, daß jeder, der eine Chipkarte der Telekom kauft, seine Personalien angeben müßte.

Offensichtlich zielt die Regelung darauf ab, jedes verfügbare Datum für eine Überwachung nutzbar zu machen. Unbeachtet blieben auch hier die bereits angeführten Konsequenzen, die das Auseinanderfallen von Dienste- und Infrastrukturanbieter für die Überwachung haben.

Mit der ENFOPOL-Entschließung werden zwar zunächst keine die Mitgliedstaaten bindenden Rechtsvorschriften geschaffen. Die freiwillige Umsetzung der Entschließung würde aber die schon dargestellte Mehrfachüberwachung eines Kommunikationsvorgangs durch eine überwachende Behörde bewirken. Dies unterstreicht nur noch einmal, wie dringend eine den technischen und organisatorischen Veränderungen im Telekommunikationssektor angepaßte **Neuregelung der Telekommunikationsüberwachung** ist. Diese Neuregelung hat Eingriffe in das Fernmeldegeheimnis zu minimieren. Dies liegt im Interesse des Grundrechtsschutzes wie im Interesse einer effektiven Arbeit der Sicherheitsbehörden und nicht zuletzt der Wettbewerbsfähigkeit der deutschen Unternehmen.

Das Internet und andere neuen Formen der Telekommunikation führen dazu, daß heute deutlich **sensiblere Daten** über Telekommunikationsnetze verschickt werden – man denke allein an die Daten, die bei Telebanking oder Telemedizin anfallen. Dem Schutz des Fernmeldegeheimnisses kommt dadurch erheblich größere Bedeutung zu. Diese gesteigerte Bedeutung aber hat bislang nicht zu einer entsprechenden Stärkung des Fernmeldegeheimnisses geführt (vgl. Tz. 2.1).

Was ist zu tun?
Die Landesregierung sollte sich dafür einsetzen, daß in einer Novellierung des TKG die Überwachung der Telekommunikation vor dem Hintergrund der Entwicklungen auf dem Telekommunikationssektor grundlegend neu bewertet wird.

7.9 Set-Top-Boxen datenschutzgerecht gestalten!

Die neuen Medien wie Internet und die herkömmlichen wie Fernsehen und Hörfunk nähern sich technisch immer mehr an. Damit entstehen auch vergleichbare datenschutzrechtliche Problemlagen. Erfreulicherweise zeichnet sich die Übernahme der vorbildlichen Multimedia-Regelungen auf den Rundfunkbereich ab.

Bei der Nutzung des **Internet** und von **Online-Diensten** sind sich viele Nutzer inzwischen der datenschutzrechtlichen Risiken bewußt. Der Gesetzgeber hat bereits im Jahr 1997 darauf reagiert und vorbildliche Regelungen zum Datenschutz im IuKDG und im Mediendienste-Staatsvertrag erlassen (vgl. 20. TB, Tz. 7.1).

Allerdings wird vielen Bürgern noch gar nicht bewußt geworden sein, daß ähnliche Probleme künftig auch im Bereich der herkömmlichen Medien Fernsehen und Hörfunk entstehen können. Der Grund dafür ist, daß auch diese Medien in absehbarer Zeit vollständig in **digitalisierter Form übertragen** werden sollen. Schon jetzt gibt es entsprechende Angebote der öffentlich-rechtlichen und der privaten Rundfunkveranstalter.

Zum Empfang des digitalisierten Rundfunks wird ein Empfangsgerät benötigt. Mit dieser **Set-Top-Box** besteht grundsätzlich auch die Möglichkeit, daß die Rundfunkveranstalter über einen Rückkanal Daten darüber sammeln, wer welche Sendungen abgerufen hat. Diese Informationen sollen beim sog. Pay-TV zur nachträglichen Bezahlung der abgerufenen Sendungen verwendet werden. Gleichzeitig würde sich auch ein detailliertes Informationsprofil des Nutzers ergeben.

> **?** ***Set-TopBox***
>
> *Die Set-Top-Box ist ein Gerät, das digitale Signale entschlüsselt und in analoge Informationen für den Fernsehbildschirm umwandelt. Dazu muß die Chipkarte des Teilnehmers im Schlitz der Box stecken. Auf der Chipkarte sind die Zugriffsberechtigungen für die verschlüsselten Sendungen und Kanäle gespeichert. Über die Chipkarte wird ebenfalls die Abrechnung abgewickelt.*

Die Inanspruchnahme des Rückkanals zu Abrechnungszwecken ist allerdings keineswegs zwingend. Die Abrechnung für die digitalen Fernsehprogramme ist auch anonym mit im voraus bezahlten **Prepaid-Karten** möglich. Auch die Inhaber von Verwertungsrechten können durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen in datenschutzgerechter Weise einen Nachweis über die zahlenmäßige Inanspruchnahme ihrer Sendungen erreichen.

Bei der anstehenden vierten Änderung rundfunkrechtlicher Staatsverträge, die voraussichtlich in der ersten Jahreshälfte 1999 erfolgen wird, ist auch die Aufnahme entsprechender Regelungen vorgesehen. Die Regelungen lehnen sich an die vorbildlichen Vorschriften des Informations- und Kommunikationsdienste-Gesetz des Bundes und den Multimedia-Staatsvertrag der Länder vom August 1997 an. Sie enthalten ebenso wie diese Regelungswerke das Gebot der **Datensparsamkeit** und die Verpflichtung für Rundfunkveranstalter, die Nutzung und Bezahlung von Rundfunkangeboten **anonym** oder unter **Pseudonym** zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Daten über die Inanspruchnahme bestimmter Sendungen dürfen nur gespeichert werden, wenn dies für die Erstellung eines Einzelnachweises erforderlich ist. Schließlich ist auch die Möglichkeit eines Datenschutz-Audits der Rundfunkveranstalter vorgesehen. Hersteller und Anbieter von Set-Top-Boxen müssen sich rechtzeitig auf diese Rechtslage einstellen und ihre Produkte entsprechend gestalten. Diese Regelungen könnten der Gefahr entgegenwirken, daß der **„Gläserne Fernsehkonsument"** in wenigen Jahren Wirklichkeit wird.

Was ist zu tun?

Das Land Schleswig-Holstein sollte nachdrücklich die geplanten datenschutzrechtlichen Bestimmungen im Rundfunkänderungsstaatsvertrag unterstützen. Hersteller von Set-Top-Boxen müssen sich rechtzeitig auf die Rechtslage einstellen.

8. Europa

EU-Richtlinie zur elektronischen Signatur

Die EU-Kommission hat zwar die Notwendigkeit erkannt, für die elektronische Signatur einen einheitlichen europäischen Rechtsrahmen vorzugeben. Wegen unterschiedlicher Vorstellungen der Mitgliedstaaten über die erforderlichen Sicherheitsstandards geriet das Vorhaben aber ins Stocken.

Seit August 1997 gibt es in Deutschland rechtliche Rahmenregelungen für die Anwendung der digitalen Signatur (19. TB, Tz. 7.7; 20. TB, Tz. 7.2 sowie oben Tz. 7.6). Auch in anderen europäischen Staaten wurden erste Schritte zur Regelung von **rechtsverbindlichen Willenserklärungen in Rechnernetzen** unternommen oder bereits Gesetze erlassen. Die Europäische Union ist nun am Zuge, einen einheitlichen Rechtsrahmen zu schaffen, um die Authentizität von elektronischen Willenserklärungen abzusichern und den grenzüberschreitenden **Electronic Commerce in Europa** zu fördern. Es soll vermieden werden, daß divergierende nationale Regelungen für den Handel im weltumspannenden Internet alleine in Europa eine Vielzahl von Signaturverfahren und Zertifikaten erforderlich machen, die der Nutzer alle bereithalten und je nachdem, in welchem Land der Server steht, einsetzen muß.

Die EU-Kommission hat Mitte des Jahres 1998 einen **Vorschlag für eine Richtlinie** des europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen (1998/C 325/04) vorgelegt. Deren Vorgaben unterscheiden sich in einigen Punkten deutlich von den Formulierungen des deutschen Signaturgesetzes und der Signaturverordnung.

Der Richtlinienvorschlag setzt auf einer abstrakteren Ebene an als die deutschen Vorschriften. Die in der Richtlinie sogenannte **elektronische Signatur** muß vier Anforderungen erfüllen:

- Sie muß ausschließlich dem Unterzeichner zugewiesen sein,
- sie muß den Unterzeichner identifizieren können,
- sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann und
- eine nachträgliche Veränderung der unterzeichneten Daten muß offenkundig werden.

Diese Anforderungen zeichnen sich durch ihre **technische Offenheit** aus. Im Unterschied zum deutschen Signaturgesetz wird damit die Möglichkeit eröffnet, auch künftig zu entwickelnde, heute noch nicht bekannte Verfahren für die elektronische Signatur einzusetzen. Zum jetzigen Zeitpunkt dürfte gleichwohl ausschließlich die im deutschen Signaturgesetz beschriebene digitale Signatur alle Voraussetzungen erfüllen.

Teilweise enthält der Richtlinienentwurf **praxisgerechtere Regelungen** als die deutschen Vorschriften. So soll es zum Beispiel möglich sein, daß ein Signaturzertifikat nicht nur an eine natürliche Person, sondern z. B. auch an eine Organisation, Behörde oder Gesellschaft ausgegeben wird. Dies erleichtert die Nutzung digitaler Signaturen in der Verwaltung.

Der Richtlinienentwurf geht insofern über die deutschen Vorschriften hinaus, als er von dem nationalen Gesetzgeber verlangt, die **elektronische Signatur** mit der **handschriftlichen Unterschrift gleichzustellen**. Dies ist problematisch, weil die elektronische Signatur nicht ohne weiteres sämtliche Funktionen erfüllt, die die Schriftform sicherstellt. So kann z. B. die mit der Schriftform häufig beabsichtigte Warnung des Erklärenden vor den möglicherweise weitreichenden Folgen seiner Willenserklärung bei der elektronischen Signatur nur über zusätzliche Softwaremodule sichergestellt werden.

Im Gegensatz zum deutschen Gesetzgeber verzichtet der Richtlinienentwurf auf die genaue Definition der Sicherheitsanforderungen, die an die Verfahren zu stellen sind. Dahinter steht die aus dem britischen Recht übernommene Idee, die erforderlichen Sicherheitsstandards würden sich am Markt von selbst durchsetzen, wenn nur – wie in dem Richtlinienentwurf – die Haftung bei Sicherheitsmängeln geregelt sei. Damit wird jedoch das entscheidende Ziel der Richtlinie verfehlt, nämlich das **Vertrauen der Anwender** in ein Verfahren der elektronischen oder digitalen Signatur zu stärken. Dies führte dazu, daß neben Deutschland die Länder Belgien, Dänemark, Frankreich, Italien, Portugal und Österreich gegen die vorliegende Entwurfsfassung stimmten. Vor allem Großbritannien, aber auch die Niederlande, Finnland und Schweden wollten dagegen an dem Entwurf festhalten. Es ist zu hoffen, daß die EU dieses wichtige Thema möglichst zügig weiterverfolgt.



Zum internationalen Stand der Regelungen zur digitalen Signatur findet sich ein ausführlicher Überblick unter *www.mbc.dom/ds_sum.html*

Was ist zu tun?

Im Rahmen seiner Einflußmöglichkeiten sollte Schleswig-Holstein, u. a. während der Zeit der deutschen Ratspräsidentschaft im ersten Halbjahr 1999, darauf hinwirken, daß Sicherheitsstandards in den Richtlinienentwurf aufgenommen werden.

9. Was es sonst noch zu berichten gibt

9.1 Polizei bereinigt zügig ihre Personalakten

Bereits im letzten Jahr (vgl. 20. TB, Tz. 4.2.10) haben wir auf eine erfolgreiche Zusammenarbeit zwischen Innenministerium und uns bei der Umstellung und der Bereinigung von Personalakten im Bereich der Landespolizei hingewiesen. Inzwischen ist die Aktion bei

- allen Polizeidirektionen,
- dem Landeskriminalamt,
- dem Polizeiverwaltungsamt,
- den Geschäftsstellen der Polizeiinspektionen Flensburg, Husum, Kiel, Rendsburg, Plön, Bad Segeberg, Itzehoe und Lübeck,
- den Polizeirevieren Flensburg, Husum, Rendsburg-Stadt, Bad Segeberg, Norderstedt, Plön und Itzehoe,
- den Polizei-Bezirksrevieren Kiel, Bad Segeberg, Plön, Itzehoe,
- dem Polizei-Autobahnrevier Neumünster,
- der Geschäftsstelle der Bezirkskriminalinspektion Itzehoe,
- der Kriminalpolizeistelle Plön,

erfolgt. Von ca. 8 650 Personalakten sind inzwischen etwa 2 000 entsprechend nach neuem Recht bereinigt und umorganisiert worden. Damit nimmt die Personalverwaltung der Polizei in diesem Bereich eine Spitzenstellung in der gesamten Landesverwaltung ein.

9.2 Neue Datenschutzregelungen im Straßenverkehrsgesetz

Anfang 1999 trat eine Neufassung des Straßenverkehrsgesetzes mit datenschutzrechtlichen Regelungen für das Führerscheinwesen in Kraft. Die Mitarbeiterinnen und Mitarbeiter der Fahrerlaubnisbehörden wurden im Hinblick auf diese neuen Vorschriften vom Verkehrsministerium in Zusammenarbeit mit unserer Dienststelle geschult. Dadurch soll zukünftig trotz der unterschiedlichen organisatorischen und personellen Strukturen in den Kreisen und kreisfreien Städten ein hohes und einheitliches Datenschutzniveau erreicht werden.

9.3 Einblick in Gutachten des Medizinischen Dienstes

Ein Vater stellte kurz vor seinem Tod bei seiner Krankenkasse einen Antrag auf Gewährung von Leistungen nach dem Pflegeversicherungsgesetz. Deshalb erstellte der Medizinische Dienst der Krankenversicherung ein Gutachten über seinen Gesundheitszustand. Etwa zur gleichen Zeit erstellte er sein Testament. Nach dem

Tod des Vaters wollte die Tochter das Gutachten einsehen, um festzustellen, ob der Vater bei der Testamentserstellung im Vollbesitz seiner geistigen Kräfte war. Die Krankenkasse verweigerte die Einsicht, weil die Tochter nicht Beteiligte im Pflegegeldverfahren des Vaters sei – zu Unrecht. Die Krankenkasse übersah, daß die Sozialdaten Verstorbener genutzt werden dürfen, wenn die schutzwürdigen Interessen des Verstorbenen oder seiner Angehörigen nicht entgegenstehen. Die Tochter hatte ein berechtigtes Interesse an der Einsicht in das medizinische Gutachten vorgebracht. Deshalb haben wir der Krankenkasse empfohlen, der Tochter das Gutachten über den verstorbenen Vater zugänglich zu machen.

9.4 Zwangsvollstreckung in der Wohngemeinschaft

Nach mehreren erfolglosen Versuchen war der Vollstreckungsbeamte einer Stadt froh, bei einem erneuten Hausbesuch überhaupt jemanden anzutreffen. Daß es sich bei der Hausbewohnerin, die die Tür öffnete, nicht um den Schuldner handelte, störte ihn nicht. Obwohl sie ihren Namen nannte und darauf hinwies, daß der Betroffene nicht zu Hause sei, trug der Vollstreckungsbeamte sein Anliegen vor und legte dabei sogar die Akte mit dem Zwangsvollstreckungsvorgang offen. Auf den Datenschutz angesprochen, erwiderte er nur: „Das ist falsch, schließlich besteht eine eheähnliche Gemeinschaft". Unabhängig von der Frage, ob er tatsächlich davon ausgehen konnte, daß beide Personen in eheähnlicher Gemeinschaft lebten, wäre damit nicht automatisch die Ermächtigung verbunden gewesen, geschützte Vollstreckungsdaten an den Partner weiterzugeben. Wegen der unbefugten Übermittlung personenbezogener Daten aus einem Vollstreckungsverfahren war gegenüber der Stadt eine Beanstandung auszusprechen.

9.5 Neufassung von MiStra und MiZi

Die bundeseinheitlichen Verwaltungsvorschriften Mitteilungen in Strafsachen bzw. in Zivilsachen (MiStra und MiZi) wurden im Berichtsjahr an die neuen gesetzlichen Übermittlungsermächtigungen nach dem Inkrafttreten des Justizmitteilungsgesetzes angepaßt. In vielen Fällen sind auf Empfehlung der Datenschutzbeauftragten Entscheidungen jetzt Richtern oder Staatsanwälten vorbehalten, um die in ihren Auswirkungen besonders bedeutsamen Mitteilungen (z. B. an den Arbeitgeber oder an eine Ordnungsbehörde) einer Einzelfallprüfung zu unterwerfen. Differenzierter als bislang sind nun auch die Voraussetzungen, der Umfang und der Zeitpunkt der Mitteilungen geregelt. Bislang fehlen noch die landesspezifischen Ergänzungen.

9.6 Datenzentrale als Privatunternehmen?

Im Zuge der Überlegungen des Landes, die Datenzentrale Schleswig-Holstein in ein Privatunternehmen umzuwandeln und eine Partnerschaft mit einem marktführenden Softwarehaus einzugehen, sind wir vom Verwaltungsrat der Datenzentrale um eine datenschutzrechtliche Stellungnahme gebeten worden. Wir haben uns dafür ausgesprochen, daß die Rechtsform der Anstalt öffentlichen Rechts erhalten

bleibt, weil dies auf Dauer für die Kunden der Datenzentrale aus dem Bereich der öffentlichen Verwaltung die zuverlässigere Lösung ist. Außerdem können nur auf diese Weise die bewährten direkten Kontroll- und Einflußmöglichkeiten des Datenschutzbeauftragten und anderer Kontrollinstanzen erhalten bleiben. Deshalb ist die Entscheidung der Landesregierung, die Rechtsform nicht zu verändern, jedoch Kooperationen mit den entsprechenden Einrichtungen in den Ländern Bayern und Hamburg einzugehen, zu begrüßen.

9.7 Klatsch über Hausdurchsuchung in einer Gemeinde

Zwei Mitarbeiter einer Amtsverwaltung sollten, wie gesetzlich vorgesehen, als Zeugen zu Hausdurchsuchungen der Polizei hinzugezogen werden. Namen und Adressen der Betroffenen erfuhren sie allerdings erst unmittelbar vor Beginn des Einsatzes. Zufällig fand eine der Durchsuchungen bei den Nachbarn eines der Mitarbeiter statt, weshalb sein Kollege dort als Zeuge fungierte. Als die Beamten dort klingelten, teilte ihnen die Hausbesitzerin mit, das ganze Dorf wisse durch Erzählungen ihres Nachbarn, daß heute irgendwo eine polizeiliche Durchsuchung stattfinde. Dies wurde allerdings von ihm bestritten und ließ sich im Rahmen unserer Kontrollbefugnisse nicht verifizieren. Fest steht jedoch aufgrund eines entsprechenden Vermerkes über die Hausdurchsuchung in der polizeilichen Ermittlungsakte, daß in der Gemeinde Informationen über bevorstehende polizeiliche Maßnahmen kursierten, die – auch wenn sie noch nicht direkt personenbezogen waren, da die Amtsverwaltung die Namen der Betroffenen noch nicht gekannt hatte – der dienstlichen Schweigepflicht unterlagen. Die Amtsverwaltung hat auf unsere Veranlassung sämtliche Mitarbeiter nochmals auf die Bedeutung der Schweigepflicht hingewiesen.

10. Rückblick

10.1 Terminsaushänge bei nichtöffentlichen Gerichtsverfahren

Schade, der Justizminister hat die Chance nicht genutzt. Im letzten Tätigkeitsbericht (Tz. 5.2) schilderten wir die Problematik, daß auch in nichtöffentlichen Verfahren die Namen der Verfahrensbeteiligten aus der Terminsrolle am Verhandlungssaal ersichtlich sind. Der Justizminister hatte zwar unseren Vorschlag zur Änderung der Aktenordnung aufgegriffen. Die Gerichte lehnten ihn aber mit der Argumentation ab, die Eintragung des Namens in die Terminsrolle sei erforderlich, damit Beteiligte zur rechten Zeit an den rechten Ort der Gerichtsverhandlung gelangen könnten. Diese Argumentation überzeugt nicht, da bereits in mehreren anderen Bundesländern auf die Nennung von Namen auf der Terminsrolle für nichtöffentliche Verfahren verzichtet wird. Wir gehen davon aus, daß auch in Schleswig-Holstein die beteiligten Parteien anhand ihrer Ladung den richtigen Verhandlungssaal finden können, wenn in den Terminsrollen nur noch das Aktenzeichen eingetragen wird. Der Justizminister sollte deshalb seinen ursprünglichen Vorschlag zur Änderung der Aktenordnung realisieren.

10.2 Nachkontrolle in einer Führerscheinstelle

Die Prüfung einer Fahrerlaubnisbehörde im Jahre 1994 hatte eine Reihe von Mängeln offenbart (vgl. 17. TB, Tz. 4.6.1). Mit einer Nachkontrolle haben wir die Umsetzung der Mängelbeseitigung überprüft. Wir stellten folgendes fest: Im Bereich der Aktenorganisation waren positiv zu bewertende Änderungen vorgenommen worden. Aber dort, wo ein größerer Personaleinsatz notwendig gewesen wäre, z. B. bei Fehlerbereinigungen, war man immer noch nicht recht vorangekommen. Unzutreffende Informationen wurden nur bereinigt, wenn der Fall ohnehin zur Bearbeitung anstand. Dies wurde mit Personalmangel begründet. Es wurde nunmehr in Aussicht gestellt, „wie in den vergangenen Jahren auch, Mitarbeiter aus anderen Sachgebieten, sofern dieses dort vertretbar ist, mit einzusetzen", um diese Arbeit möglichst umgehend zu erledigen. Der Zusatz: „Ob dieses dann entsprechend Ihrem Vorschlag gelingt, bleibt abzuwarten", wird eine weitere Nachprüfung zur Folge haben.

10.3 Datensicherheit bei der Justiz

Im 18. Tätigkeitsbericht (Tz. 4.4.3) hatten wir auf Sicherheitsmängel bei der Aufbewahrung von Prozeßakten in Gerichten hingewiesen. Der Grund hierfür lag in der ungenügenden Ausstattung der Gerichte mit verschließbaren Schränken. Wegen fehlender Haushaltsmittel erfolgte zunächst nur eine zögerliche Mängelbeseitigung. Nun ist allmählich Abhilfe in Sicht. Im Haushalt 1998 waren bereits 120 000 DM für die Beschaffung von abschließbaren Registraturschränken ausgewiesen. Auch für 1999 ist ein Betrag in gleicher Größenordnung vorgesehen.

10.4 Neuer Erlaß regelt die Aufbewahrungsfristen von Bußgeldakten

Im 20. Tätigkeitsbericht berichteten wir über Prüfungen in Bußgeldstellen, die für die Ahndung von Verkehrsordnungswidrigkeiten zuständig sind (vgl. Tz. 4.6.2). Wir kritisierten, daß die Aktenvorgänge in den jeweiligen Bußgeldstellen unterschiedlich und vor allem unangemessen lange aufbewahrt wurden. Im März 1998 hat das Verkehrsministerium nunmehr die Aufbewahrung von Bußgeldakten neu geregelt und angemessene Aufbewahrungsfristen festgelegt.

10.5 Fahrtenbücher von Ärzten und Apothekern

Seit Jahren streiten die Datenschutzbeauftragten des Bundes und der Länder mit den Steuerverwaltungen über die Notwendigkeit, die Namen der Patienten bzw. Kunden von Ärzten und Apothekern in den Fahrtenbüchern für beruflich/geschäftlich und privat genutzte Kraftfahrzeuge zu vermerken (vgl. 19. TB, Tz. 4.10.3). Vor kurzem ist Bewegung in die starre Front der Finanzministerien gekommen. Sie werden sich offenbar künftig mit Aufzeichnungen ohne Namensnennung begnügen. Ärzte, Apotheker, Steuerberater usw. sollten sich hierauf berufen.

10.6 KomFIT – ein neuer Name, ein neues Konzept

Die Automationskommission der kommunalen Landesverbände hat nach fast dreißigjährigem Bestehen ihre Arbeit beendet und ist durch ein neues Gremium ersetzt worden, das den Namen „Kommunales Forum für Informationstechnik – KomFIT" trägt. Es wird sich „projektorientierter" als bisher mit den Fragen der Informations- und Kommunikationstechniken im kommunalen Bereich befassen. Dies bedingt einen personellen Neuanfang und eine organisatorische Lösung von der Datenzentrale. Auch in dem neuen Gremium sind wir mit beratender Stimme vertreten. KomFIT wird aufgrund der Tatsache, daß nunmehr auch ein hauptamtlicher Koordinator tätig ist, insbesondere die von uns seit Jahren geforderte Zertifizierung von IT-Produkten für den kommunalen Markt zügig vorantreiben können (vgl. 13. TB, Tz. 6.3; 19. TB, Tz. 6.3; 20. TB, Tz. 6.2).

10.7 Staatskanzlei startet Pilotprojekt für Telearbeit

Unsere Vorschläge zur datenschutzgerechten Gestaltung von Telearbeitsplätzen (vgl. 20. TB, Tz. 6.4) sind offenbar auf fruchtbaren Boden gefallen. Die Staatskanzlei, die derzeit ein interministerielles Pilotprojekt zur Einführung von Telearbeit betreibt, hat uns als Berater in die Projektgruppe eingeladen. Unsere Sicherheitsanforderungen sollen bei der Gestaltung der einzelnen Pilotarbeitsplätze ihren Niederschlag finden.

10.8 Landesinitiative Informationsgesellschaft

„Schleswig-Holstein als Modellregion – wofür?", unter dieser Überschrift hatten wir im 20. Tätigkeitsbericht (Tz. 2.1) über die Aktivitäten Schleswig-Holsteins im Rahmen der „Regional Information Society Initiative" (RISI) der Europäischen Union berichtet. Wir stellten die Frage, wodurch sich Schleswig-Holsteins Weg in die Informationsgesellschaft unverwechselbar von dem anderer Länder unterscheiden sollte. Zugleich berichteten wir von vier Vorschlägen, die wir im Rahmen unserer Mitarbeit bei RISI gemacht haben. Inzwischen hat sich folgendes getan:

- Wir hatten vorgeschlagen, in die Verfassung einen Artikel „Teilhabe an der Informationsgesellschaft" einzufügen. Hierfür gab es keine 2/3-Mehrheit im Parlament, aber die aus RISI hervorgegangene Landesinitiative hat sich das Motto gegeben: „Informationsgesellschaft für alle".
- Die Einrichtung eines Lehrstuhls zu Fragen der Informationsgesellschaft hat das Hochschulministerium inzwischen abgelehnt.
- Die Installation eines Servers, der den anonymen Zugang zum Internet ermöglichen soll, kann demnächst beginnen. Die Landesinitiative bewilligte Mittel für ein entsprechendes Modellprojekt, an dem unsere Dienststelle beteiligt ist.
- Die Modernisierung der Arbeit der Datenschutzbeauftragten wurde im Rahmen der Sommerakademie '98 breit diskutiert. Eine Reihe von konkreten Modernisierungsschritten sind bei uns selbst inzwischen eingeleitet.

Über die weiteren Projekte der Landesinitiative Informationsgesellschaft entscheidet nunmehr eine Arbeitsgruppe, in der eine Reihe von Ministerien, die Kommunen und wir mit Sitz und Stimme vertreten sind.

11. Einige Beispiele dafür, was die Bürger von unserer Tätigkeit haben

Datenschutzbeauftragte haben die Aufgabe zu kontrollieren und zu kritisieren, wenn sie Mängel bei der Verarbeitung personenbezogener Daten feststellen. Auch in diesem Bericht ist an vielen Stellen von „Kritik", „Bedenken", „Beanstandung" u. ä. die Rede. Dies könnte zu dem Schluß führen, Kritik und Behinderung seien unsere Hauptaufgaben. In Wirklichkeit geht es um Verbesserungen zugunsten des Grundrechtsschutzes der Bürgerinnen und Bürger. Hier einige Beispiele aus dem vergangenen Jahr, in denen dies gelungen ist.

1. *Das neue Insolvenzrecht sieht vor, daß private Stellen Schuldenbereinigungsverfahren durchführen. Durch eine Gesetzeslücke wäre der Schutz der dabei verwendeten hochsensiblen Daten unzureichend gewesen. Auf unsere Intervention beschloß der Landtag eine wirksame Datenschutzregelung zugunsten der Schuldner.*

2. *Bei der Veröffentlichung von Planfeststellungsbeschlüssen wurden die Namen der Einwender genannt. Dadurch konnte sich jeder über die Gegner von Planprojekten informieren. In Zukunft werden Ziffern verwendet.*

3. *Im Rahmen von Stundungsverfahren wurden bislang sensible Daten von Gebührenschuldnern aufgrund einer unpräzisen Generalklausel erhoben. Nunmehr wurden die Verwaltungsvorschriften präzisiert. Die Betroffenen werden außerdem künftig über die Verwendung der Daten „von Amts wegen" informiert.*

4. *Die Bundesregierung plante, den Großen Lauschangriff auch gegen Ärzte, Psychologen, Journalisten und andere zur Verschwiegenheit verpflichtete Berufsgruppen zuzulassen. Bei Gesprächen mit Ärzten, Psychologen usw. hätten sich die Bürgerinnen und Bürger nicht mehr auf die Vertraulichkeit verlassen können. Auch wir haben dazu beigetragen, daß das Gesetz nunmehr Ausnahmen für die genannten Berufsgruppen vorsieht.*

5. *Im Rahmen des Personalinformationssystems PERMIS werden sensible Personaldaten auf Leitungswegen übertragen. Ein unbefugtes Abhören durch Dritte hätte weitreichende Folgen für die betroffenen Bediensteten haben können. Nunmehr sollen die Personaldaten entsprechend unserer Empfehlung nur noch verschlüsselt übertragen werden.*

6. *Bei der Behandlung von Bauleitplänen in öffentlicher Sitzung wurden auch Namen genannt. Auf diesem Wege konnten z. B. höchstpersönliche Gründe für Einwendungen publik werden. Ein neuer Erlaß des Innenministers stellt jetzt sicher, daß Einwendungen öffentlich nicht mehr namensbezogen erörtert werden.*

7. *Bei einigen Polizeistationen wurden Ausdrucke aus Dateien zu den Akten genommen. Spätere Änderungen, z. B. Löschungen in den Dateien, hätten so unterlaufen werden können. Diese Praxis wurde abgestellt.*

8. *Das Verfahren MEGA bei den Gerichten war bislang so gestaltet, daß es Bedienungsfehler erleichterte, die zur versehentlichen Eintragung in die Schuldnerliste führen konnten. Die Folgen für die Betroffenen waren fatal, weil die Schuldnerlisten auch an Banken, Auskunfteien etc. gelangen. Nach unserer Kontrolle wurde MEGA so verbessert, daß es nicht mehr zu einem derartigen Erfassungsfehler beiträgt.*

9. *Bislang verlangte das Finanzamt von Ärzten, daß sie die Namen von Patienten in ihre Fahrtenbücher eintrugen. Dies bedeutete eine unnötige Belastung der Patienten. Nunmehr wurden die Bestimmungen so geändert, daß die Erfassung der Patientennamen entfällt.*

10. *Im staatsanwaltschaftlichen System MESTA sollten die Beendigungsgründe von Strafverfahren nicht präzise genug vermerkt werden. Da die Polizei ihre Datenspeicherungen anhand der Verfahrensausgänge bei der Justiz überprüfen muß, hätte dies zu Unklarheiten und insbesondere verlängerten Speicherfristen bei der Polizei geführt. Wie von uns vorgeschlagen, werden die Gründe für den Verfahrensausgang jetzt präzise erfaßt, so daß die Polizei ihre Kriminalakten gezielt bereinigen kann.*

11. *Immer mehr Kommunen organisieren auf unseren Vorschlag ihre Datenhaltung so, daß personenbezogene Daten nur zentral in gut gesicherten Servern und nicht in den einzelnen PC gespeichert werden. Damit sinkt z. B. das Risiko, daß sensible Daten beim Diebstahl von PC (allein im letzten Jahr sollen insgesamt ca. 100 PC aus Behörden gestohlen worden sein) in falsche Hände geraten.*

12. *Bei einer Polizeistation war es üblich, daß der Stadt eine Unbedenklichkeitsbescheinigung über jeden Obdachlosen ausgestellt wurde, der in der Stadt übernachten wollte. Nach unserer Kontrolle wurde das Verfahren eingestellt.*

13. *Die Daten über Strafverfahren sollten im Rahmen des neuen Dateiverfahrens MESTA zunächst zwischen den beteiligten Staatsanwaltschaften unverschlüsselt ausgetauscht werden. Jetzt hat sich der Justizminister unserer Auffassung angeschlossen, daß diese sensiblen Daten nur verschlüsselt übermittelt werden dürfen.*

14. *Bislang wurden Buchprüfer, die in einem Strafverfahren zur Unterlassung ihrer Tätigkeit verurteilt wurden, namentlich in den Kammermitteilungen der Steuerberaterkammer bekanntgegeben. Jetzt wurde dieser „elektronische Pranger" eingestellt.*

15. *In manchen Sozialämtern herrschte Unklarheit, in welchem Umfang von Antragstellern Kontoauszüge verlangt werden dürfen. Die Folge waren oft pauschale, zu weit gehende Anforderungen. In einer Veröffentlichung im Amtsblatt haben wir für alle Sozialämter präzise Hinweise gegeben, in welchem Umfang Hilfeempfänger Kontoauszüge einreichen müssen.*

16. *Immer wieder verlangten Wohngeldstellen die Vorlage von Vermieterbescheinigungen. Vielen Wohngeldempfängern war es peinlich, ihren Vermietern ihre finanzielle Situation zu offenbaren, manche wollten lieber auf das Wohngeld verzichten. Wir haben erreicht, daß die Betroffenen die notwendigen Nachweise auch in anderer Form beibringen können.*

17. *Ziehen Sozialhilfeempfänger um, werden häufig die kompletten Sozialhilfeakten routinemäßig an den neuen Wohnort geschickt. Dadurch werden unter Umständen mehr Sozialdaten übermittelt als wirklich notwendig. Im Amtsblatt haben wir Hinweise veröffentlicht, die es den Sozialbehörden erleichtern sollen, nur die erforderlichen Daten zu übermitteln.*

18. *Bislang wurden bei der Aktenführung der Versorgungsausgleichskasse Personalakten nicht von anderen Vorgängen getrennt. Die Betroffenen hatten so nicht die Möglichkeit, ihr Akteneinsichtsrecht auszuüben. Nach unserer Prüfung wurden die Unterlagen neu geordnet, so daß zu jeder Person eine eigene Personalakte geführt wird.*

19. *In der Vergangenheit mußten die Kommunen die Versorgungsausgleichskasse über alle bedeutsamen Personalvorgänge ihrer aktiven Beamten unterrichten, auch wenn dies für versorgungsrechtliche Zwecke nicht notwendig war. Dies führte zu umfangreichen „Zweitakten", in denen nicht erforderliche Daten gespeichert waren. Nach unserer Intervention wurde der Umfang der Datenübermittlungen auf das erforderliche Maß reduziert.*

20. *Obwohl bei der Beihilfegewährung mit dem Bescheid alle Belege, die Diagnosedaten enthalten, an die Betroffenen zurückgegeben werden müssen, fanden sich in verschiedenen Fällen solche Unterlagen in den Beihilfeakten der Versorgungsausgleichskasse. Dadurch entstanden hochsensible Vorgänge mit Gesundheitsdaten über Kommunalbedienstete. Nach unserer Prüfung sind die Sachbearbeiterinnen und Sachbearbeiter ausdrücklich auf die Rückgabepflicht hingewiesen worden, so daß künftig keine Diagnosedaten mehr in Beihilfeakten gespeichert werden dürften.*

21. *Bislang gab es keine Regelungen für die Verarbeitung von Schüler- und Elterndaten im häuslichen Bereich der Lehrkräfte. Vor allem beim Einsatz privater PC war die Datensicherheit nicht immer gewährleistet, so daß Daten über Schüler und ihre Eltern Unbefugten zur Kenntnis gelangen konnten. Nach unserer Beratung erließ das Bildungsministerium Hinweise zur sicheren Verarbeitung der Daten.*

22. *Durch unzureichende personelle und organisatorische Abschottung im polizeiärztlichen Dienst war es im System angelegt, daß Daten aus der vertraulichen hausärztlichen Behandlung in dienstrechtliche Begutachtungen einflossen. Auf unsere Intervention hin erfolgt jetzt eine Reorganisation des Dienstes, die der ärztlichen Schweigepflicht gerecht wird.*

23. *Bei Forschungsprojekten mit teilweise sehr persönlichen Daten, war immer wieder festzustellen, daß die Betroffenen beim Einholen von Einwilligungen nicht ausreichend oder gar falsch über die Datenverarbeitung informiert wurden. Die Folge waren ungenügende Transparenz und fehlende Akzeptanz. Bei vielen Projekten, z. B. einem gemeinsamen Projekt der Medizinischen Universität Lübeck und des Verbands der Deutschen Rentenversicherungen, führte unsere Beratung zu einer präzisen Information der Betroffenen, bevor sie über ihre Einwilligung entschieden.*

12. DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN



Die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN besteht inzwischen seit sechs Jahren. Das Interesse an den Kursen, Seminaren und Workshops ist ungebrochen, so daß die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN ihre Unkosten selbst tragen kann und nicht auf Haushaltsmittel angewiesen ist. Insgesamt wurden bislang 128 Kurse mit etwa 3 000 Teilnehmern durchgeführt.

Nach wie vor versteht sich die DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN als Bündelung und Rationalisierung der Beratungsaktivitäten des Landesbeauftragten für den Datenschutz und als Ergänzung der Kontrolltätigkeit. Der Abdruck des Logos der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN an verschiedenen Stellen dieses Berichts macht diesen Zusammenhang deutlich. Das Jahresprogramm 1999 beruht auf den Erfahrungen mit den bisherigen Programmen und berücksichtigt neue Entwicklungen im Datenverarbeitungsrecht und in der Computertechnik.

Das Jahresprogramm 1999 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN mit näheren Informationen zu den einzelnen Kursen, Seminaren und Workshops sowie 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
Homepage: www.schleswig-holstein.datenschutz.de

Das Programm ist auch im Internet auf unserer Homepage (Rubrik: Datenschutzakademie) verfügbar.

Terminübersicht für die Kurse der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN 1999

Kurse/Seminare/Workshops	Kurz-bez.	Zeit	Ort
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	SI 5	15.03.-17.03.1999	Leck
Datenschutz an der Schule	L 18	29.03.1999	Kiel – KYC
Datenschutz im Ordnungsamt	O 5	20.04.1999	Kiel – KYC
Technik und Recht von Firewalls	FW 3	21.04.1999	Kiel – KYC
Neue Methoden der Datensicherheit	CEB 1	22.04.1999	Kiel – KYC
Datenschutz im Bauamt	B 3	26.04.1999	Kiel – KYC
Schutz von Personaldaten	P 7	06.05.-07.05.1999	Bordesholm
Behördliche Datenschutzbeauftragte	D 9	17.05.-21.05.1999	Leck
Verschlüsselung und digitale Signatur	VS 2	27.05.1999	Kiel – KYC
Datenschutz in Netzen	EN 3	01.06.1999	Kiel – KYC
Internet für Behörden	INT 3	02.06.1999	Kiel – KYC
Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 4	08.06.1999	Kiel – KYC
Technischer Datenschutz an Schulen	LT 1	16.06.1999	Kiel – KYC
Einführungskurs Kommunalbereich	EK 5	01.07.1999	Kiel – KYC
Datenschutz an der Schule	L 19	08.07.1999	Kiel – KYC
Einstieg in das Datenschutzrecht	E 6	13.07.1999	Kiel – KYC
Beauftragte für Sozialdatenschutz	S 7	30.08.-03.09.1999	Leck
Führung von Personalakten	PA 7	06.09.-07.09.1999	Bordesholm
Datenschutz in Netzen	EN 4	07.09.1999	Kiel – KYC
Internet für Behörden	INT 4	08.09.1999	Kiel – KYC
Datenschutz an der Schule	L 20	16.09.1999	Kiel – KYC
Personalrat und Einführung von IT-Systemen	PI 1	21.09.1999	Kiel – KYC
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 6	30.09.1999	Bordesholm
Behördliche Datenschutzbeauftragte	D 10	04.10.-08.10.1999	Leck
Workshop für behördliche Datenschutzbeauftragte	DW 3	12.10.1999	Kiel – KYC
Workshop zur Datensicherheit	SIW 4	04.11.-05.11.1999	Leck
Modernisierung in der Verwaltung	MV 1	09.11.1999	Kiel – KYC
Datenschutz an der Schule	L 21	18.11.1999	Kiel – KYC
Einführungskurs Kommunalbereich	EK 6	25.11.1999	Kiel – KYC
Einstieg in das Datenschutzrecht	E 7	07.12.1999	Kiel – KYC
Technik und Recht von Firewalls	FW 4	08.12.1999	Kiel – KYC

13. Sommerakademie 1999

Die Sommerakademie 1999 findet am

23. August 1999

im Landeshaus in Kiel statt. Das Thema lautet:

„Polizei und Datenschutz"
- Neupositionierung im Zeichen der Informationsgesellschaft -

Die Sommerakademie 1999 möchte mit der Wahl dieses Themas das manchmal schwierige Verhältnis zwischen Polizei und Datenschutz beleuchten. Auf keinem anderen Feld des Datenschutzes hat es in den vergangenen Jahren so viele Auseinandersetzungen gegeben wie im Bereich der polizeilichen Datenverarbeitung. Informationeller Selbstbestimmung scheint die polizeiliche Datenerhebung geradezu diametral entgegenzustehen, da sie in der Regel ohne Zustimmung der Betroffenen und häufig genug heimlich erfolgt. Die Konflikte der vergangenen Jahre drehten sich zumeist um die Schaffung und konkrete Ausgestaltung der Rechtsgrundlagen für die polizeiliche Datenverarbeitung. Die Sommerakademie 1999 möchte die Entwicklung der Gesetzgebung analysieren und der Frage nachgehen, ob die neuen Befugnisnormen zu restriktiv oder zu allgemein formuliert sind. Polizei und Datenschutz ziehen nämlich durchaus unterschiedliche Bilanzen aus diesen Kontroversen und sehen häufig jeweils in der „anderen Seite" denjenigen, der sich unangemessen durchgesetzt hat.

Die Sommerakademie wird aber ebenso die konkrete Praxis des Datenschutzes und der Datensicherheit im polizeilichen Alltag behandeln. Dabei wird es darum gehen, ob der Datenschutz tatsächlich dem Erfolg polizeilichen Handelns im Wege steht, welche Resultate mit den neuen gesetzlichen Eingriffsbefugnissen erzielt worden sind und ob es zuverlässige Methoden gibt, die Effizienz der polizeilichen Arbeit zu untersuchen. Auf der Tagesordnung steht dabei auch eine kritische Analyse von Erfolgen und Mißerfolgen der Datenschutzbeauftragten im Polizeibereich.

Die Sommerakademie wird diese Fragen auf dem Hintergrund der Veränderungen der Informationstechnik behandeln und untersuchen, welche Folgerungen aus den Bedingungen der modernen Informationsgesellschaft für Polizei und Datenschutz zu ziehen sind. Polizeipraktiker, Wissenschaftler, Datenschützer und Publizisten werden in einer offenen Diskussion versuchen, neue Ansätze für „Polizei und Datenschutz" zu finden, die bei der Forderung nach immer neuen Rechtsgrundlagen nicht stehenbleiben. Im Kern geht es um die grundlegende Problematik, welchen Stellenwert polizeiliche Effizienz im Rechtsstaat haben soll und damit um den fundamentalen verfassungsrechtlichen Abwägungsprozeß zwischen Freiheit und Eingriff.

An der Vorbereitung und Durchführung der Sommerakademie 1999 wirken u. a. mit:

Heinz-Werner **Arens**, Präsident des Schleswig-Holsteinischen Landtages; Dr. Wolfgang **Bär**, Richter am Amtsgericht Bayreuth; Dr. Johann **Bizer**, Wissenschaftlicher Assistent am Institut für Öffentliches Recht der Johann Wolfgang Goethe-Universität, Frankfurt am Main; Eike **Bleibtreu**, Bundesvorsitzender Bund Deutscher Kriminalbeamter, Bonn; Prof. Dr. Hans Peter **Bull**, Professor für Öffentliches Recht und Verwaltungslehre an der Universität Hamburg; ehem. Innenminister des Landes Schleswig-Holstein; ehem. Bundesbeauftragter für den Datenschutz; Dr. Ann **Cavoukian**, Information und Privacy Commissioner, Ontario, Canada; Simon **Davies**, Director of Privacy International, Brighton, United Kingdom; Prof. Dr. Erhard **Denninger**, Professor für Öffentliches Recht II und Rechtsphilosophie an der Johann Wolfgang Goethe-Universität, Frankfurt am Main; Dr. Alexander **Dix**, Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg: Prof. Dr. Hansjürgen **Garstka**, Berliner Datenschutzbeauftragter; Prof. Dr. Walter **Gropp**, Professor für Strafrecht und Strafprozeßrecht an der Justus-Liebig-Universität, Gießen; Dr. Horst **Herold**, Präsident des Bundeskriminalamtes a. D.; Eberhard **Kempf**, Rechtsanwalt und Notar, Frankfurt; Vorsitzender des Strafrechtsausschusses des Deutschen Anwaltsvereins; Dr. Ulrich **Kersten**, Präsident des Bundeskriminalamtes, Wiesbaden; Prof. Dr. Hans F. **Lisken**, Polizeipräsident a. D.; Honorarprofessor an der Heinrich-Heine-Universität, Düsseldorf; Yves **Michels**, Saarländisches Ministerium des Innern, Saarbrücken; Projektkoordinator des Kooperationsvorhabens „Qualitätsverbesserung der Polizeiarbeit" der Bertelsmann Stiftung; Prof. Wolf-Dieter **Narr**, Freie Universität zu Berlin; Kay **Nehm**, Generalbundesanwalt; Thomas **Petri**, Wissenschaftlicher Assistent an der Johann Wolfgang Goethe-Universität, Frankfurt am Main; Prof. Dr. Gerd **Pfeiffer**, Bundesgerichtshofspräsident a. D.; Heribert **Prantl**, Süddeutsche Zeitung, München; Dr. Norbert **Pütter**, Wissenschaftlicher Assistent an der Freien Universität zu Berlin; Prof. Fritz **Sack**, Professor für Kriminologie an der Universität Hamburg; Dr. rer. nat. Peter M. **Schneider**, Hochschuldozent am Institut für Rechtsmedizin der Johannes Gutenberg-Universität, Mainz; Dr. Hans-Hermann **Schrader**, Hamburgischer Datenschutzbeauftragter; Bettina **Sokol**, Landesbeauftragte für den Datenschutz in Nordrhein-Westfalen; Norbert **Spinrath**, Bundesvorsitzender Gewerkschaft der Polizei, Hilden; Prof. Dr. Albert **von Mutius**, Professor für Öffentliches Recht und Verwaltungslehre an der Christian-Albrechts-Universität zu Kiel; Vorsitzender des Kuratoriums der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN; Hartmut **Wegener**, Staatssekretär im Innenministerium des Landes Schleswig-Holstein; Ulrich **Werner**, Referent beim Hamburgischen Datenschutzbeauftragten; Dr. Ekkehard **Wienholtz**, Innenminister des Landes Schleswig-Holstein; Jörg **Ziercke**, Leiter der Polizeiabteilung im Innenministerium des Landes Schleswig-Holstein; 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

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

Tätigkeitsbericht
des letzten Jahres als Landtagsdrucksache

Tätigkeitsberichte
der letzten Jahre als Sammlung

Landtagsdrucksache 14/1738
Bericht über die Notwendigkeit der Novellierung des Landesdatenschutzgesetzes mit dem Gesetzentwurf des Landesbeauftragten für den Datenschutz, Begründung zum Gesetzentwurf, Synopse LDSG-alt/ LDSG-neu und weiteren Materialien

Faltblatt
Safer Surfen!: Verschlüsseln - Ich?

Diverse Aufkleber
Der Mensch ist mehr als Null und Eins
Aufkleber zum Thema Verschlüsselung

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 1999

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). Zur Zeit sind das Bundes- und Landesdatenschutzgesetz und die Datenschutzverordnung, der Text zum Entwurf des neuen Landesdatenschutzgesetzes, das Programm der DATENSCHUTZAKADEMIE, Informationen zu den Sommerakademien, die Tätigkeitsberichte der letzten Jahre, Pressemitteilungen und weitere Publikationen im elektronischen Format abrufbar. Weiterhin ist dort der öffentliche Schlüssel des Landesbeauftragten für den Datenschutz und ein benutzerfreundliches Verschlüsselungsprogramm für vertrauliche E-Mail-Kommunikation erhältlich.

Datenschutz auf CD-ROM
Der Landesbeauftragte für den Datenschutz hat eine CD-ROM mit dem Inhalt der zum Zeitpunkt der Veröffentlichung dieses Berichtes auf der Homepage bereitstehenden Informationen herausgebracht. Für Benutzer, die über kein eigenes Programm verfügen, um die internetgerechten Dateien anzuschauen, wird ein einfacher Offline-Browser mitgeliefert. Als Systemvoraussetzung sind ein PC 386/486 oder höher, mindestens 12 MB Hauptspeicher, MS-DOS 5.0 aufwärts und Windows 3.1, Windows für Workgroups bzw. Windows 95/NT erforderlich. Die CD-ROM kann beim Landesbeauftragten kostenlos angefordert werden.

Anhang

Die Vorschläge zur Novellierung des Landesdatenschutzgesetzes auf einen Blick

Mit Beschluß vom 3. September 1998 beauftragte der Schleswig-Holsteinische Landtag den Landesbeauftragten für den Datenschutz mit der Erstellung eines Berichts zur Notwendigkeit der Novellierung des Landesdatenschutzgesetzes. Dabei sollen konkrete Vorschläge anhand einiger im Beschluß aufgeführter Kriterien gemacht werden. Im wesentlichen geht es um folgende Gesichtspunkte:

Am 24. Oktober 1995 haben das Europäische Parlament und der Rat der Europäischen Union die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**EG-Datenschutzrichtlinie**) erlassen. Die Richtlinie hat das Ziel, das Datenschutzniveau innerhalb der Europäischen Union zu vereinheitlichen, um den freien Datenverkehr im Gebiet der Union zu erleichtern. Sie hätte bis zum 24. Oktober 1998 durch den nationalen Gesetzgeber umgesetzt werden müssen. Damit ist auch der schleswig-holsteinische Gesetzgeber verpflichtet, das Landesdatenschutzgesetz umgehend an die Richtlinie anzupassen. Seit der letzten Neufassung des Landesdatenschutzgesetzes im Jahre 1991 hat es eine stürmische Weiterentwicklung der **Datenverarbeitungstechnik** gegeben. So ist beispielsweise das Internet zu einem massenhaft genutzten Kommunikationsmedium geworden, an dem zunehmend auch Verwaltungsbehörden als Informationsanbieter oder Nutzer teilhaben. Generell haben die Automatisierung der Datenverarbeitung im Lande und die Vernetzung der eingesetzten Systeme in den vergangenen Jahren stetig zugenommen. Es wurden völlig neue Datenbank-, Client-Server-, Kommunikations- und Chipkartensysteme entwickelt, die mehr und mehr auch in Schleswig-Holstein zur Anwendung kommen. Diese neuen technischen Entwicklungen bedrohen aber nicht nur die Privatsphäre der Bürger; sie können auch dazu genutzt werden, den Datenschutz praktisch umzusetzen. Diese **datenschutzfreundlichen Technologien** finden im Datenschutzrecht bislang keine Berücksichtigung.

Die Akzeptanz des Datenschutzrechts litt in den letzten Jahren zunehmend daran, daß die Vorschriften immer komplizierter geworden und gelegentlich nur noch schwer verständlich sind. Diese Defizite sind bei der Novellierung des Landesdatenschutzgesetzes möglichst zu beheben. Das Ziel muß es sein, ein **praktikables Datenschutzrecht** für eine moderne, serviceorientierte Verwaltung zu schaffen, ohne daß dabei der Schutz der Bürgerrechte aufgeweicht wird. Der Vorschlag für ein novelliertes Landesdatenschutzgesetz (LDSG-E) versucht auf folgende Weise, diesen Anforderungen gerecht zu werden:

1. Umsetzung der EG-Datenschutzrichtlinie:

Entsprechend den Vorgaben der Richtlinie werden sogenannte **sensible Daten** einem besonderen Schutz unterstellt. Es handelt sich dabei z. B. um Daten über die Gesundheit, über die rassische oder ethnische Herkunft oder über politische Meinungen. Nach § 10 Abs. 4 LDSG-E dürfen diese Daten nur auf der Grundlage bereichsspezifischer Vorschriften verarbeitet werden.

Nach der Richtlinie ist es unzulässig, die Betroffenen nachteiligen **Entscheidungen** zu unterwerfen, die ohne menschliches Zutun in einem **automatisierten Verfahren** getroffen wurden, bei dem bestimmte Aspekte der Person der Betroffenen bewertet wurden. Diese Regelung ist in § 19 LDSG-E umgesetzt.

Als ein neues Rechtsinstitut zum Schutze der Betroffenen sieht die Richtlinie ein sog. **Widerspruchsrecht** vor. Es kommt dann zum Tragen, wenn die Datenverarbeitung zwar rechtmäßig ist, sich jedoch aus besonderen persönlichen Konstellationen eine Unzumutbarkeit für den Betroffenen ergibt. Der Entwurf setzt diese Vorgabe in § 29 LDSG-E unter der Bezeichnung „Einwand gegen die Datenverarbeitung" um.

In Übereinstimmung mit der Richtlinie darf die **Datenübermittlung** an öffentliche und nichtöffentliche Stellen in den Mitgliedstaaten der EU unter denselben Voraussetzungen wie innerhalb eines Mitgliedstaates erfolgen. Die Übermittlung in **Drittstaaten** ist grundsätzlich nur zulässig, wenn dort ein angemessenes Datenschutzniveau herrscht. Die Einzelheiten dazu regelt § 15 LDSG-E.

Die Richtlinie schreibt eine sogenannte **Vorabkontrolle** der Datenverarbeitung vor. Dabei sollen solche Verarbeitungen präventiv geprüft werden, die besondere Gefährdungen für die Rechte der Betroffenen mit sich bringen können. Nach § 5 Abs. 3 LDSG-E dürfen diese Verfahren nur eingesetzt werden, wenn die Vorabkontrolle ergeben hat, daß Rechtsverletzungen mit hinreichender Sicherheit ausgeschlossen sind.

Die Richtlinie legt den Umfang der **Benachrichtigung des Betroffenen** bei der Datenerhebung sowie den Umfang des Auskunftsrechts fest. Diese Regelungen sind in den §§ 26 und 27 LDSG-E zusammengefaßt.

In Übereinstimmung mit der Richtlinie ist in § 9 LDSG-E geregelt, daß die Bestellung eines **internen Datenschutzbeauftragten** bei der datenverarbeitenden Stelle die Meldepflicht für automatisierte Verfahren beim Landesbeauftragten für den Datenschutz entfallen läßt. Eine dezentralisierte und praxisnahe Kontrolle kann deutliche Vorteile haben. Dabei wird diese Lösung jedoch nicht zwingend vorgeschrieben. Die Stellen können auf die Bestellung eines Datenschutzbeauftragten auch verzichten, unterliegen dann aber weiterhin der Meldepflicht.

Für den Fall, daß die automatisierte Datenverarbeitung zu Schäden bei den Betroffenen führt, sieht die Richtlinie eine **Beweislastverteilung** zu Lasten der datenverarbeitenden Stelle vor. Dies wird in § 30 Abs. 4 LDSG-E umgesetzt.

2. Berücksichtigung der Veränderungen in der Datenverarbeitungstechnik

Die bisherigen „10 Gebote" zur Datensicherheit in § 7 Abs. 2 LDSG sind an der Großrechnertechnologie orientiert. § 6 Abs. 1 LDSG-E faßt die **Ziele der Datensicherheit** übersichtlich zusammen, die bei jeder Form der Datenverarbeitung beachtet werden müssen.

Informationen zwischen Bürgern und Behörden werden künftig auch über das **Internet** ausgetauscht werden. Aus diesem Grund wird in § 11 Abs. 3 LDSG-E die Möglichkeit vorgesehen, die datenschutzrechtliche Einwilligung statt in der grundsätzlich vorgeschriebenen Schriftform nach Wunsch auch elektronisch abzugeben. Die Einzelheiten der Regelung lehnen sich an die Vorschriften des Multimediarechts an.

Auch in der öffentlichen Verwaltung werden immer häufiger Konzepte, die durch Schlagworte wie **papierloses Büro** oder **Workflow-Management** beschrieben werden, in die Praxis umgesetzt. § 7 Abs. 5 LDSG-E sieht in den Fällen, in denen Daten ausschließlich automatisiert gespeichert werden, eine spezielle Protokollierung vor. § 17 Abs. 5 LDSG-E soll zudem sicherstellen, daß die einzelnen Abteilungen einer Organisation, die auf ein solches System zugreifen, ihre Pflichten und Verantwortlichkeiten klar fassen und gegeneinander abgrenzen.

In Zukunft werden voraussichtlich die Fälle zunehmen, in denen **mehrere datenverarbeitende Stellen** gemeinsam mit demselben Datenbestand arbeiten. Für diese Fälle werden in § 17 LDSG-E die Verantwortlichkeiten und Pflichten der beteiligten Stellen klar geregelt und abgegrenzt. Es sind besondere Protokollierungspflichten vorgesehen, um die Überprüfbarkeit der Verfahren sicherzustellen, § 7 Abs. 4 LDSG-E.

Die heutigen **Chipkarten** stellen miniaturisierte Hochleistungscomputer dar, bei deren Einsatz vor allem die Transparenz für die Betroffenen verlorenzugehen droht. § 18 LDSG-E schreibt deshalb vor, daß bei den Anwendungen im öffentlichen Bereich die Transparenz erhalten bleiben muß.

In die bestehende Regelung zur **Videoüberwachung** und **Videoaufzeichnung** ist nunmehr eingefügt, daß die Aufzeichnungen im Regelfall nach sieben Tagen gelöscht werden müssen, § 20 LDSG-E.

3. Reaktion auf die Modernisierungsbestrebungen in der Verwaltung

Schon nach der bestehenden Datenschutzverordnung ist die **Freigabe** Voraussetzung dafür, daß ein automatisiertes Verfahren eingesetzt werden darf. Die Freigabe wird nun wegen ihrer überragenden Bedeutung für das Verwaltungsverfahren (Zurechenbarkeit von Verwaltungshandeln, Haftung für die Folgen der Datenverarbeitung), aber auch um ihre besondere Bedeutung für eine ordnungsgemäße und sichere Datenverarbeitung zu unterstreichen, im Gesetz selbst geregelt. Voraussetzung für die Freigabe ist nach § 5 Abs. 2 LDSG-E vor allem, daß ein

klares Sicherheitskonzept für die geplante Datenverarbeitung vorliegt, daß das Verfahren rechtmäßig ist und daß es getestet wurde.

§ 3 Abs. 1 Nr. 2 LDSG-E weitet den Anwendungsbereich des Landesdatenschutzgesetzes auch auf solche Stellen aus, die zwar **privatrechtlich organisiert** sind, die jedoch im wesentlichen öffentlich-rechtlichen Stellen „gehören". Das LDSG soll anwendbar sein, wenn diese Organisationen Aufgaben der öffentlichen Verwaltung wahrnehmen. Damit soll verhindert werden, daß der Grundrechtsschutz der Bürgerinnen und Bürger absinkt, wenn öffentliche Aufgaben in einer privaten Rechtsform erbracht werden.

Die Verwaltung bedient sich im Rahmen des **Outsourcing** zunehmend externen Sachverstands, um ihre Aufgaben zu erfüllen. Beispiele dafür sind Wartung oder sonstige Betreuung von IT-Systemen. Außerdem werden für Teilaufgaben immer häufiger externe Sachverständige und Gutachter hinzugezogen. Hierfür fehlte bisher eine datenschutzgerechte Regelung. § 16 Abs. 4 und Abs. 5 LDSG-E erklären die Regelungen der Auftragsdatenverarbeitung für entsprechend anwendbar. Die externen Sachverständigen und Gutachter haben die Pflicht, nach Erfüllung ihrer Aufgabe die Daten zu löschen und/oder an die datenverarbeitende Stelle zurückzugeben.

Im Zuge der Verwaltungsmodernisierung kommen zunehmend „papierlose" Verfahren und Workflow-Konzepte zum Einsatz. § 7 Abs. 5 und §17 Abs. 5 LDSG-E regeln, auf welche Weise die **Revisionsfähigkeit** des Verwaltungshandelns sichergestellt werden muß.

§ 10 Abs. 5 LDSG-E schreibt vor, daß die **Datenverarbeitung** von vornherein so zu **organisieren** ist, daß bei Datenübermittlungen oder Auskunftsersuchen der Betroffenen nicht umständliche und aufwendige Trennungsarbeiten vorgenommen werden müssen. Diese Regelung erlangt eine besondere Bedeutung, falls ein allgemeines Informationszugangsrecht eingeführt wird.

Die zunehmende Automatisierung der Datenverarbeitung im Rahmen der Verwaltungsmodernisierung führt zu immer mehr Einwirkungsmöglichkeiten der **Systemadministratoren**. § 7 Abs. 2 LDSG-E schreibt eine spezielle Protokollierung ihrer Aktivitäten vor.

Zunehmend werden auch bei öffentlichen Stellen in Schleswig-Holstein die neuen Formen der **Telearbeit** diskutiert. § 7 Abs. 3 LDSG-E soll im Interesse der Bürgerinnen und Bürger für diese Fälle einen Datensicherheitsstandard bewirken.

4. Grundsatz der Datenvermeidung und Datensparsamkeit

Datenvermeidung und Datensparsamkeit werden durch die Regelungen in § 4 LDSG-E für die Verwaltung verbindliche Ziele, vor allem bei der **Auswahl von IT-Produkten**. Durch die Verpflichtung zur Nachfrage nach entsprechenden Produkten soll für die Anbieter ein Anreiz zu ihrer Entwicklung gegeben werden.

Eine besondere Bedeutung für die Erreichung des Ziels der Datensparsamkeit hat die **Anonymisierung**, die in § 2 Abs. 4 LDSG-E neu definiert worden ist. Die im Vergleich zum geltenden LDSG flexiblere Definition führt dazu, daß die Anonymisierung früher erreicht wird und damit leichter im Dienste des Datenschutzes eingesetzt werden kann. § 22 Abs. 1 LDSG-E sieht z. B. vor, daß bei allen Planungen zur Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke zunächst die Möglichkeit der Anonymisierung geprüft werden muß. Nur wenn dies nicht möglich ist, darf auf die in der Vorschrift aufgeführten Rechtsgrundlagen zurückgegriffen werden.

Die **Pseudonymisierung** ist in § 2 Abs. 5 LDSG-E gesetzlich definiert. Von der Anonymisierung unterscheidet sie sich dadurch, daß eine Zuordnungsfunktion existiert, mit der der Personenbezug wiederhergestellt werden kann. Hat eine Stelle keinen Zugriff auf diese Zuordnungsfunktion, so ist ihr die Verwendung der Daten ohne weiteres gestattet, § 10 Abs. 6 LDSG-E. In besonderem Maße kann die wissenschaftliche Datennutzung von der Pseudonymisierung profitieren, wie sich aus § 22 Abs. 2 und 3 LDSG-E ergibt.

5. Datenschutz durch Technik

Die Vorschriften über Datenschutz durch Technik sind in einem eigenen Abschnitt unter der Bezeichnung „**Systemdatenschutz**" zusammengefaßt und ihrer Bedeutung entsprechend nach den allgemeinen Vorschriften plaziert.

Die in § 5 LDSG-E erstmals in das Gesetz aufgenommene Freigabe automatisierter Verfahren darf nur erteilt werden, wenn in einem **Sicherheitskonzept** dargelegt ist, in welcher Weise die Datensicherheitsmaßnahmen umgesetzt werden sollen.

Für automatisierte Verfahren werden in § 7 LDSG-E einzelne Maßnahmen zur **Datensicherheit verbindlich** vorgeschrieben

Die Grundsätze der **Datenvermeidung** und der **Datensparsamkeit** sollen über das Erforderlichkeitsprinzip hinaus bereits bei der Auswahl und Gestaltung von Verfahren und Produkten zu einer Reduzierung der Risiken beitragen, vgl. § 4 LDSG-E.

Nach § 10 Abs. 5 Satz 1 LDSG-E ist die **Datenverarbeitung** so zu **organisieren**, daß eine Selektierung der Daten nach der jeweiligen Erforderlichkeit ohne weiteres möglich ist. In dieser Beziehung haben moderne Datenbanksysteme entscheidende Vorteile gegenüber den üblichen Akten und Verwaltungsvorgängen.

Eine Schlüsseltechnik für den Datenschutz ist die **Kryptographie**. Aufgrund der generellen Unsicherheit bei der Übertragung von Daten im Internet muß sich der Bürger selbst durch Verschlüsselung schützen können. Aber auch bei dem Transport von Verwaltungsinformationen ist die Verschlüsselung ein probates Instrument für die Datensicherheit. Eine entsprechende Regelung findet sich in § 7 Abs. 3 LDSG-E. In § 2 Abs. 6 LDSG-E ist die Verschlüsselung erstmals in einem

Datenschutzgesetz definiert.

6. Neue Instrumente des Datenschutzes

Nach § 34 Abs. 3 LDSG-E soll es den öffentlichen Stellen ermöglicht werden, ihr Datenschutz- und Datensicherheitskonzept durch den Landesbeauftragten für den Datenschutz vorab bewerten zu lassen. Nach einem positiven Ergebnis dieses **Audit-Verfahrens** können die öffentlichen Stellen davon ausgehen, daß die automatisierte Verarbeitung von der Konzeption und der vorgesehenen Implementierung her unbedenklich ist.

§ 4 Satz 2 LDSG-E verpflichtet die öffentlichen Stellen, bei der **Beschaffung** solchen **IT-Systemen** den Vorzug zu geben, „deren Vereinbarkeit mit den Vorschriften des Datenschutzes und den Regeln der Datensicherheit in einem förmlichen Verfahren festgestellt wurde". Die in einem solchen Verfahren künftig vergebenen Prädikate sollen Bestandteil der Beschaffungskriterien für die öffentlichen Stellen des Landes Schleswig-Holstein werden. Dies ist für die vielen kleineren Organisationseinheiten im kommunalen Bereich von besonderer Bedeutung.

§ 34 LDSG-E enthält eine Reihe von **Beratungsaufgaben** für die oder den Landesbeauftragten für den Datenschutz. Verstärkt sind vor allem die Bürgerinnen und Bürger über Fragen des Datenschutzes und der Datensicherheit zu beraten. Die bereits jetzt durchgeführten umfangreichen Schulungs- und Fortbildungsveranstaltungen werden als Aufgabe in das Gesetz aufgenommen. Zugleich wird die Möglichkeit eröffnet, für einige dieser Aufgaben eine **Refinanzierung** über Gebühren zu ermöglichen.

7. Verschlankung und Entbürokratisierung

In § 2 LDSG-E wird der **Begriff der Datenverarbeitung** nunmehr in einer besser verständlichen Weise definiert. Von den ursprünglichen acht Phasen der Datenverarbeitung finden sich in der neuen **Definition** nur noch die vier wichtigsten. Die Regelung wurde dadurch beträchtlich verschlankt.

Wegen der im öffentlichen Bereich ohnehin weitgehend spezialgesetzlich geregelten Geheimhaltungspflichten war das **Datengeheimnis** nach § 6 LDSG alter Fassung verzichtbar.

Zur Entbürokratisierung und Dezentralisierung der Datenschutzkontrolle trägt es bei, wenn die öffentlichen Stellen von der Möglichkeit Gebrauch machen, einen **internen Datenschutzbeauftragten** zu bestellen, § 9 LDSG-E. In diesem Fall sind sie nämlich nicht verpflichtet, die bei ihnen betriebenen automatisierten Verfahren an den Landesbeauftragten für den Datenschutz zu melden.

In § 10 Abs. 2 LDSG-E ist nunmehr eine **bereichsübergreifende Rechtsgrundlage** für die Verarbeitung nicht besonders sensibler Daten enthalten. Dadurch entfällt künftig die Notwendigkeit, in derartigen Fällen mehr oder weniger

gleichlautende Datenverarbeitungsbestimmungen in eine Vielzahl von Fachgesetzen, Verordnungen oder Satzungen aufzunehmen.

Im Interesse der Konzentration auf das Wesentliche erleichtert § 10 Abs. 3 LDSG-E die Verarbeitung von **Daten**, die aus **allgemein zugänglichen Quellen** entnommen werden können.

In § 13 Abs. 2 LDSG-E ist die **Abgrenzung der Verantwortlichkeiten** bei Datenübermittlungen zwischen öffentlichen Stellen sprachlich klarer gefaßt worden.

Bisher durften **automatisierte Übermittlungsverfahren**, mit denen es einer Stelle möglich ist, die bei einer anderen Stelle gespeicherten Daten direkt abzurufen, nur auf der Grundlage einer eigens dafür erlassenen Rechtsverordnung eingerichtet werden. Nunmehr ist der Einsatz solcher Verfahren nach einer Prüfung der materiellen Voraussetzungen des § 17 LDSG-E ohne vorherigen Erlaß einer Rechtsverordnung zulässig.

Die Bestimmung über das **Fernmessen und Fernwirken** wurde in § 21 LDSG-E deutlich verschlankt. Die Teile der Vorschrift, die sich bereits aus allgemeinen datenschutzrechtlichen Normen ergeben, wurden gestrichen.

Bei der **Datenverarbeitung zu wissenschaftlichen Zwecken** kann künftig in vielen Fällen darauf verzichtet werden, die Genehmigung der Aufsichtsbehörde einzuholen, wenn die Daten anonymisiert oder pseudonymisiert worden sind, § 22 LDSG-E. Die Voraussetzungen dafür sind deutlich erleichtert worden.

Die Vorschrift, mit der die **Verarbeitung von Personaldaten** für öffentlich Bedienstete geregelt wird, § 23 LDSG-E, wurde auf das Wesentliche reduziert.

Die bisher im Zusammenhang mit der Datenerhebung geregelte **Aufklärung** bzw. **Benachrichtigung der Betroffenen** ist nun in § 26 LDSG-E im Abschnitt über die Rechte der Betroffenen am thematisch richtigen Regelungsort untergebracht und zusammengefaßt.

Vereinfacht wurden auch die Vorschriften über die **Auskunftsrechte der Betroffenen**, § 27 LDSG-E.

Eine deutliche Deregulierung stellt auch der **Verzicht** auf **Strafvorschriften** im LDSG dar. Diese waren schon bisher subsidiär zu anderen Strafnormen des Informationsrechts. Fälle, in denen Verurteilungen nach § 33 LDSG a.F. erfolgten, sind nicht bekanntgeworden. Aus diesen Gründen erschien es ausreichend, Verstöße gegen das Datenschutzrecht lediglich als Ordnungswidrigkeiten zu verfolgen.

Um unnötigen Gesetzgebungsaufwand in einer Reihe von Fachgesetzen infolge der Entbehrlichkeit des Dateibegriffs zu vermeiden, wurde in § 36 LDSG-E **übergangsweise** noch der **Dateibegriff** aufgenommen.

8. Verbesserung des Schutzes des informationellen Selbstbestimmungsrechts

In § 1 LDSG-E wird deutlicher die **grundrechtliche Fundierung** der gesetzlichen Aufgaben des Datenschutzes zum Ausdruck gebracht.

Die **Ausdehnung des Anwendungsbereiches** des Gesetzes nach § 3 Abs. 1 Nr. 2 LDSG-E schützt die Bürgerinnen und Bürger künftig auch im Falle einer Aufgabenverlagerung auf privatrechtlich organisierte Stellen.

Die nach § 5 LDSG-E erforderliche **Freigabe** vor dem Beginn der automatisierten Datenverarbeitung sichert im Interesse der Bürgerinnen und Bürger die Einhaltung eines datenschutzgerechten Standards der Ordnungsmäßigkeit und Sicherheit. Entsprechendes gilt für die einzelnen, z.T. neu geschaffenen Maßnahmen der Datensicherheit, z. B. §§ 5 und 7 Abs. 4 LDSG-E.

Die Arbeit behördlicher Datenschutzbeauftragter mit eigenen, gesetzlich geregelten Befugnissen führt zur **effektiveren Wahrnehmung** der Datenschutzaufgabe vor Ort und verbessert damit den Schutzstandard für die Betroffenen. Diese haben die Möglichkeit, sich direkt an den behördlichen Beauftragten zu wenden, § 9 Abs. 3 Satz 4 LDSG-E.

Das Konzept der dreigestuften Zulässigkeitsvoraussetzungen für die Datenverarbeitung nach § 10 LDSG-E behandelt die Daten entsprechend ihrer Sensibilität und Bedeutung und ermöglicht es, das Schutzniveau jeweils angemessen zu definieren. Daten, die weniger gefährdend sind, sind für die öffentlichen Stellen leichter verfügbar. Die sensiblen Daten dagegen sind stärker geschützt. Damit soll eine **Konzentration auf das Wesentliche** erreicht werden.

Der Schutz der Betroffenen bei der **Übermittlung** der Daten in **Drittstaaten** orientiert sich an der Richtlinie und sieht nach § 15 LDSG-E vor, daß die Datenübermittlung nur zulässig ist, wenn im Empfängerstaat ein angemessenes Datenschutzniveau existiert.

Die besonderen Verpflichtungen, die nach § 16 Abs. 5 LDSG-E bei der Datenübermittlung an **externe Gutachter** und **Sachverständige** von den öffentlichen Stellen vertraglich fixiert werden müssen, führen zu einer verbesserten Sicherung der Daten der Bürgerinnen und Bürger bei Weitergabe ihrer Daten an diese privaten Stellen.

Bei **gemeinsamen Verfahren**, bei denen mehrere Stellen mit demselben Datenbestand arbeiten, haben die Bürger künftig die Möglichkeit, ihre Rechte nach Wahl bei einer der beteiligten Stellen wahrzunehmen, § 17 Abs. 4 LDSG-E. Diese muß, wenn sie im Einzelfall nicht verantwortlich für die Speicherung ist, das Auskunftsersuchen an die zuständige Stelle weiterleiten.

Erstmalig geregelt ist die Verarbeitung von personenbezogenen Daten auf **Chipkarten** und anderen mobilen Datenverarbeitungssystemen. Die Vorschrift des

§ 18 LDSG-E soll die Rechte der Betroffenen vor allem dadurch wahren, daß die **Transparenz** derartiger Verfahren sichergestellt wird.

In Übereinstimmung mit der Richtlinie sind solche Verfahren grundsätzlich verboten, bei denen **automatisiert** und nach der Bewertung bestimmter Merkmale von Personen eine für diese nachteilige **Entscheidung getroffen** werden soll, § 19 LDSG-E.

Die **Speicherungsdauer** bei **Video-Aufzeichnungen** wurde definiert und auf eine kurze Frist von sieben Tagen begrenzt, § 20 LDSG-E.

Die Datenverarbeitung zu **wissenschaftlichen Zwecken** ist unter erleichterten Voraussetzungen zulässig, wenn die Daten anonymisiert oder wenigstens pseudonymisiert sind, § 22 LDSG-E. Dies trägt zum Schutz der Betroffenen bei, da die forschenden Stellen den Informationsgehalt der Daten nicht einzelnen Personen zuordnen können.

Bei der Auskunft an die Betroffenen stand es bisher im Ermessen der datenverarbeitenden Stelle, ob den Betroffenen anstelle der Auskunft **Akteneinsicht** gewährt wird. Nunmehr sollen die Betroffenen das Recht haben, nach ihrem Willen Auskunft oder Einsicht in die Speicherung zu erhalten, § 27 Abs. 2 LDSG-E.

In Konstellationen, in denen die Gefährdung besonderer persönlicher Interessen die Datenverarbeitung im Einzelfall unzumutbar erscheinen läßt, können die Betroffenen nach § 29 LDSG-E **Einwand** gegen die Datenverarbeitung erheben.

Kommt es durch eine unzulässige oder unrichtige automatisierte Datenverarbeitung zu Schäden an Rechtsgütern des Betroffenen, so hatte dieser bisher die Schwierigkeit, die Ursächlichkeit der Fehler für den Schaden nachzuweisen, weil das Verfahren in der Sphäre der datenverarbeitenden Stelle betrieben wurde und für ihn nur schwer nachvollziehbar war. In Übereinstimmung mit der Richtlinie ändert § 30 Abs. 4 LDSG-E die **Beweislastverteilung** zugunsten des Bürgers. Nunmehr hat die datenverarbeitende Stelle sich zu entlasten, will sie dem Schadensersatzanspruch entgehen.

Auch die umfangreichen **Beratungspflichten** der oder des Landesbeauftragten für den Datenschutz gegenüber den Bürgerinnen und Bürgern verbessern deren Rechtsposition, insbesondere ihre Möglichkeit, sich **selbst wirksam** gegen Datenmißbrauch zu **schützen**, § 34 LDSG-E.

Vorschlag des Landesbeauftragten für den Datenschutz zur Novellierung des Landesdatenschutzgesetzes

Abschnitt I:
Allgemeine Vorschriften

§ 1 Gesetzeszweck
§ 2 Begriffsbestimmungen
§ 3 Anwendungsbereich

Abschnitt II:
Systemdatenschutz

§ 4 Datensparsamkeit, Anonymisierung, Pseudonymisierung
§ 5 Freigabe automatisierter Verfahren, Vorabkontrolle
§ 6 Allgemeine Maßnahmen zur Datensicherheit
§ 7 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren
§ 8 Verfahrensverzeichnis
§ 9 Die oder der Beauftragte für den Datenschutz

Abschnitt III:
Zulässigkeit der Datenverarbeitung

§ 10 Zulässigkeit der Datenverarbeitung
§ 11 Form der Einwilligung
§ 12 Erheben, Zweckbindung
§ 13 Datenübermittlung innerhalb des öffentlichen Bereichs
§ 14 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs
§ 15 Datenübermittlung an ausländische Stellen

Abschnitt IV:
Besondere Formen der Datenverarbeitung

§ 16 Verarbeitung personenbezogener Daten im Auftrag, Wartung
§ 17 Gemeinsame Verfahren
§ 18 Mobile personenbezogene Datenverarbeitungssysteme
§ 19 Verbot automatisierter Einzelentscheidungen
§ 20 Video-Überwachung und -Aufzeichnung
§ 21 Fernmessen und Fernwirken

Abschnitt V:
Besondere Zwecke der Datenverarbeitung

§ 22 Datenverarbeitung für wissenschaftliche Zwecke
§ 23 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
[*§ 24 Besondere Dokumentationsstelle für Sekten*]

Abschnitt VI:
Rechte der Betroffenen

§ 25 Rechte der Betroffenen
§ 26 Aufklärung, Benachrichtigung
§ 27 Auskunft an Betroffene
§ 28 Berichtigung, Löschung, Sperrung
§ 29 Einwand gegen die Verarbeitung
§ 30 Schadensersatz

Abschnitt VII:
Die oder der Landesbeauftragte für den Datenschutz

§ 31 Berufung und Rechtsstellung
§ 32 Kontrollaufgaben
§ 33 Beanstandungen
§ 34 Serviceaufgaben

Abschnitt VIII:
Übergangs- und Schlußvorschriften

§ 35 Ordnungswidrigkeiten
§ 36 Übergangsvorschriften
§ 37 Inkrafttreten

Abschnitt I
Allgemeine Vorschriften

§ 1
Gesetzeszweck

Zweck dieses Gesetzes ist es, bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen die Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung, zu wahren.

§ 2
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene oder Betroffener).

(2) Datenverarbeitung ist die Verwendung personenbezogener Daten. Dabei ist

1. Erheben das Beschaffen von Daten,
2. Speichern das Aufbewahren von Daten auf Datenträgern,
3. Übermitteln das Weitergeben von Daten an Dritte oder der Abruf von zum Abruf bereitgehaltenen Daten durch Dritte,
4. Löschen das Unkenntlichmachen gespeicherter Daten.

(3) Datenverarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Absatz 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt.

(4) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(5) Pseudonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6) Verschlüsseln ist das Verändern von Daten derart, daß ohne Nutzung des Geheimnisses die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.

§ 3
Anwendungsbereich

(1) Dieses Gesetz gilt für öffentliche Stellen. Öffentliche Stellen im Sinne dieses Gesetzes sind

1. Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung,
2. Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen einem oder mehreren der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Beteiligt sich eine Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 2 Nr. 2 Anwendung findet, an weiteren Vereinigungen des privaten Rechts, so findet Satz 2 Nr. 2 entsprechende Anwendung.

(2) Für öffentlich-rechtliche, der Aufsicht des Landes unterstehende Unternehmen mit eigener Rechtspersönlichkeit, die am Wettbewerb teilnehmen und nicht Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten von diesem Gesetz nur § 23 und Abschnitt VII. Im übrigen gelten für sie die Vorschriften des Bundesdatenschutzgesetzes für nichtöffentliche Stellen. Die Sätze 1 und 2 gelten nicht für die Datenzentrale Schleswig-Holstein.

(3) Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor.

Abschnitt II
Systemdatenschutz

§ 4
Datenvermeidung und Datensparsamkeit

Bei der Gestaltung von Verfahren und der Auswahl von informationstechnischen Produkten zum Einsatz in automatisierten Verfahren hat die datenverarbeitende Stelle den Grundsatz der Datensparsamkeit zu beachten. Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden.

§ 5
Freigabe automatisierter Verfahren, Vorabkontrolle

(1) Der erstmalige Einsatz oder die Änderung von automatisierten Verfahren zur Verarbeitung personenbezogener Daten bedarf der Freigabe durch die Leiterin oder den Leiter der datenverarbeitenden Stelle oder eine Person, der diese Befugnis ausdrücklich übertragen worden ist. Die Verarbeitung personenbezogener Daten in automatisierten Verfahren ist erst zulässig, wenn die Freigabe erteilt worden ist. Die Freigabe ist zu dokumentieren.

(2) Die Freigabe darf nur erteilt werden, wenn

1. die rechtliche Zulässigkeit der Verarbeitung festgestellt wurde,
2. eine Dokumentation des Verfahrens vorliegt, die mindestens die in das Verzeichnis nach § 8 aufzunehmenden Angaben enthält,
3. die einzusetzenden Verfahren getestet worden sind und
4. in einem Sicherheitskonzept dargelegt ist, in welcher Weise die nach den §§ 6 und 7 erforderlichen technischen und organisatorischen Maßnahmen umgesetzt werden.

(3) Im Rahmen der Freigabe von automatisierten Verfahren hat die datenverarbeitende Stelle zu prüfen, ob von den Verfahren eine besondere Gefährdung für die Rechte der Betroffenen ausgehen kann. Ist dies der Fall, so darf das Verfahren nur eingeführt oder wesentlich geändert werden, wenn die Gefährdung durch technische oder organisatorische Maßnahmen wirksam beherrscht werden kann. Bei der Beurteilung dieser Frage ist die oder der Beauftragte für den Datenschutz nach § 9 oder die oder der Landesbeauftragte für den Datenschutz zu beteiligen.

(4) Die Landesregierung regelt durch Verordnung die Einzelheiten der Freigabe nach Absatz 2, insbesondere

1. die über Absatz 2 Nummer 2 hinausgehenden Anforderungen an die Dokumentation automatisierter Verfahren,
2. Kriterien für Verfahren, deren Freigabe unter vereinfachten Voraussetzungen erfolgen kann,
3. das Vorgehen beim Test von Programmen,
4. die Anforderungen an das Sicherheitskonzept und
5. die Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen.

Dabei sind die in den §§ 6 und 7 genannten Maßnahmen der Datensicherheit nach dem Stand der Technik fortzuschreiben. Die oder der Landesbeauftragte für den Datenschutz ist zu beteiligen.

§ 6
Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, daß personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können,
3. zu gewährleisten, daß festgestellt werden kann, welche personenbezogenen Daten wann von wem verarbeitet worden sind.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind.

§ 7
Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) Automatisierte Verfahren sind so zu gestalten, daß eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.

(2) Zugriffe, mit denen Änderungen an freigegebenen automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(3) Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die datenverarbeitende Stelle hat sicherzustellen, daß sie die Daten entschlüsseln kann.

(4) Werden bei gemeinsamen Verfahren nach § 17 personenbezogene Daten übermittelt, so

sind die Empfänger, der Zeitpunkt der Übermittlung und die jeweils übermittelten Daten zu protokollieren. Die Protokolldatenbestände sind ein Jahr zu speichern.

(5) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Absatz 4 Satz 2 gilt entsprechend. Es ist sicherzustellen, daß die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind.

(6) Die datenverarbeitenden Stellen haben technische und organisatorische Maßnahmen zu treffen, um die Verarbeitung personenbezogener Daten in nicht freigegebenen automatisierten Verfahren zu unterbinden.

(7) Die datenverarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

§ 8
Verfahrensverzeichnis

(1) Die datenverarbeitende Stelle erstellt für jedes von ihr betriebene automatisierte Verfahren eine Verfahrensbeschreibung. Diese enthält Angaben über

1. Zweckbestimmung und Rechtsgrundlage des Verfahrens,
2. den Kreis der Betroffenen,
3. die Kategorien der verarbeiteten Daten,
4. die Personen und Stellen, die Daten erhalten oder erhalten können einschließlich der Auftragnehmenden,
5. geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union,
6. die datenschutzrechtliche Beurteilung der oder des behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt,
7. die eingesetzte Hard- und Software und
8. eine allgemeine Beschreibung der zur Einhaltung der Datensicherheit getroffenen Maßnahmen.

(2) Die Verfahrensbeschreibung nach Absatz 1 ist der oder dem Landesbeauftragten für den Datenschutz vor Beginn der Verarbeitung zu übersenden. Änderungen sind ihr oder ihm umgehend mitzuteilen.

(3) Die oder der Landesbeauftragte für den Datenschutz führt ein Verzeichnis der Meldungen nach Absatz 2. Das Verzeichnis kann von jeder Person eingesehen werden; dies gilt nicht für die Angaben nach Absatz 1 Nummern 7 und 8. Satz 2 gilt nicht für Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,
2. der Gefahrenabwehr oder der Strafverfolgung oder
3. der Steuerfahndung dienen,

soweit die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar hält.

(4) Von der Meldung nach Absatz 2 kann abgesehen werden, wenn bei der datenverarbeitenden Stelle eine Beauftragte oder ein Beauftragter für den Datenschutz nach § 9 bestellt ist. In diesen Fällen führt die datenverarbeitende Stelle ein Verzeichnis der bei ihr betriebenen automatisierten Verfahren. Absatz 2 und Absatz 3 Satz 2 und 3 gelten entsprechend.

§ 9
Die oder der Beauftragte für den Datenschutz

(1) Die datenverarbeitende Stelle kann schriftlich eine Beauftragte oder einen Beauftragten für den Datenschutz bestellen. Mehrere datenverarbeitende Stellen können gemeinsam eine Beauftragte oder einen Beauftragten für den Datenschutz bestellen.

(2) Die oder der Beauftragte für den Datenschutz muß die erforderliche Sachkunde und Zuverlässigkeit besitzen. Sie oder er darf durch die Bestellung keinem Konflikt mit anderen dienstlichen Aufgaben ausgesetzt sein.

(3) Die oder der Beauftragte für den Datenschutz ist unmittelbar der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu unterstellen. Sie oder er ist bei der Ausübung des Amtes weisungsfrei und darf wegen der Wahrnehmung des Amtes nicht benachteiligt werden. Sie oder er ist zur Erfüllung der Aufgaben des Amtes im erforderlichen Umfang freizustellen und mit den notwendigen Mitteln auszustatten. Beschäftigte und Betroffene können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an sie oder ihn wenden. Die oder der Beauftragte für den

Datenschutz darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. § 32 Absatz 4 gilt entsprechend.

(4) Die oder der Beauftragte für den Datenschutz überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der datenverarbeitenden Stelle. Sie oder er hat insbesondere

1. vor der Einführung oder Änderung automatisierter Verfahren ihre oder seine datenschutzrechtliche Beurteilung abzugeben,
2. zu überprüfen, ob die datenschutzrechtlichen Vorschriften eingehalten werden und ob der Einsatz automatisierter Verfahren im Rahmen der Freigabe erfolgt; Verstöße sind der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu melden,
3. die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken,
4. die Beschäftigten der datenverarbeitenden Stellen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
5. das Verzeichnis nach § 8 Absatz 4 Satz 2 zu führen und zur Einsicht bereitzuhalten.

Abschnitt III: Zulässigkeit der Datenverarbeitung

§10 Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. die oder der Betroffene eingewilligt hat,
2. eine diesem Gesetz vorgehende Rechtsvorschrift
3. oder dieses Gesetz sie erlaubt

und bei automatisierten Verfahren die Freigabe nach § 5 vorliegt.

(2) Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, soweit sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der datenverarbeitenden Stelle erforderlich ist.

(3) Die Verarbeitung personenbezogener Daten, die allgemein zugänglichen Quellen entnommen werden können, sowie von Daten, die die Betroffenen selbst zur Veröffentlichung bestimmt haben, ist über die Fälle von Absatz 2 hinaus zulässig, soweit nicht schutzwürdige Belange der Betroffenen beeinträchtigt sind.

(4) Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ist nur nach Rechtsvorschriften, die diesem Gesetz vorgehen, sowie nach § 16 Absatz 5 und den §§ 22 bis 24 dieses Gesetzes zulässig. Dasselbe gilt für Daten über strafbare Handlungen und Entscheidungen in Strafsachen. Die in den Sätzen 1 und 2 genannten Daten dürfen ausnahmsweise nach den Vorschriften dieses Abschnitts verarbeitet werden, wenn die oder der Betroffene eingewilligt hat oder soweit die Verarbeitung

1. ausschließlich im Interesse der oder des Betroffenen liegt,
2. sich auf Daten bezieht, die die oder der Betroffene selbst öffentlich gemacht hat,
3. zur Geltendmachung rechtlicher Ansprüche vor Gericht erforderlich ist oder
4. für die Abwehr von Gefahren für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter erforderlich ist.

(5) Die Datenverarbeitung soll so organisiert sein, daß bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der oder des Betroffenen überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(6) Pseudonymisierte Daten dürfen von solchen Stellen verarbeitet werden, die keinen Zugriff auf die Zuordnungsfunktion haben. Die Übermittlung pseudonymisierter Daten ist zulässig, wenn die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.

§ 11
Form der Einwilligung

(1) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. In den Fällen des § 10 Absatz 4 muß sich die Einwilligung ausdrücklich auf die dort aufgeführten Daten beziehen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die oder der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(2) Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

(3) Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, daß

1. sie nur durch eine eindeutige und bewußte Handlung der oder des Betroffenen erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihre Urheberin oder ihr Urheber erkannt werden kann und
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird.

§ 12
Erheben, Zweckbindung

(1) Personenbezogene Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. Ohne Kenntnis der Betroffenen dürfen personenbezogene Daten nur erhoben werden, wenn die Voraussetzungen von Absatz 3 Nr. 1, 2 oder 4 vorliegen. Die Herkunft der Daten ist zu dokumentieren.

(2) Personenbezogene Daten dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind. Daten, von denen die öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für die Zwecke weiterverarbeitet werden, für die sie erstmals rechtmäßig gespeichert worden sind.

(3) Die Verarbeitung für andere Zwecke ist ohne Einwilligung der oder des Betroffenen nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt,
2. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechtspositionen einzelner dies gebietet,
3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
4. die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, daß die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde.

Für Daten im Sinne von § 10 Absatz 4 findet Satz 1 Nummer 3 und 4 keine Anwendung.

(4) Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke. Die Verarbeitung zu Ausbildungs- und Prüfungszwecken hat in anonymisierter oder pseudonymisierter Form zu erfolgen. Lassen sich die in Satz 2 genannten Zwecke durch anonymisierte oder pseudonymisierte Datenverarbeitung nicht erreichen, so ist die Zweckänderung zulässig, soweit berechtigte Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

(6) Werden Daten innerhalb einer datenverarbeitenden Stelle zu einem anderen Zweck als dem nach Absatz 2 weiterverarbeitet, so ist dies zu dokumentieren.

§ 13
Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Bei der Übermittlung personenbezogener Daten an andere öffentliche Stellen sind die Voraussetzungen des § 10 Absatz 2 und des § 12 Absätze 2 bis 5 zu beachten.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Soll die Übermittlung auf Ersuchen einer Stelle erfolgen, so hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben. Die übermittelnde Stelle prüft die Schlüssigkeit der Anfrage. Bestehen im Einzelfall Zweifel, so prüft sie auch die Rechtmäßigkeit des Ersuchens. Die empfangende Stelle trägt im übrigen die Verantwortung für die Zulässigkeit der Übermittlung.

§ 14
Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

1. von diesen ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind oder
2. die Voraussetzungen des § 10 Absatz 2 vorliegen

und die Anforderungen des § 12 Absätze 2 bis 5 eingehalten werden.

(2) Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden.

§ 15
Datenübermittlung an ausländische Stellen

(1) Die Zulässigkeit der Übermittlung an öffentliche und nichtöffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes richtet sich nach den §§ 13 und 14. Die Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Vor der Entscheidung über die Angemessenheit des Datenschutzniveaus ist die oder der Landesbeauftragte für den Datenschutz zu hören.

(2) Fehlt es an einem angemessenen Datenschutzniveau, so ist die Übermittlung nur zulässig, wenn

1. die oder der Betroffene in die Übermittlung eingewilligt hat,
2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,
3. die Übermittlung zur Wahrung lebenswichtiger Interessen der oder des Betroffenen erforderlich ist,
4. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt oder
5. die oder der Landesbeauftragte für den Datenschutz die Übermittlung genehmigt, nachdem sie oder er sich davon überzeugt hat, daß die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der in § 1 genannten Rechte bietet.

(3) Die empfangende Stelle ist darauf hinzuweisen, daß die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

Abschnitt IV
Besondere Formen der Datenverarbeitung

§ 16
Verarbeitung personenbezogener Daten im Auftrag, Wartung

(1) 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 Weitergabe der Daten von der datenverarbeitenden Stelle an die Auftragnehmenden gilt nicht als Übermittlung im Sinne von § 2 Absatz 2 Nr. 3.

(2) Die datenverarbeitende Stelle hat dafür Sorge zu tragen, daß personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der nach den §§ 6 und 7 notwendigen technischen und orga-

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

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

(4) Die Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der datenverarbeitenden Stelle gilt als Datenverarbeitung im Auftrag im Sinne von Absatz 1 Satz 1.

(5) Zur Durchführung von beratenden oder begutachtenden Tätigkeiten im Auftrag der datenverarbeitenden Stelle ist die Übermittlung personenbezogener Daten an solche Personen zulässig, die durch besondere Rechtsvorschriften zur Verschwiegenheit verpflichtet sind. Die übermittelnde Stelle hat diese Personen zu verpflichten,

1. die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind, sowie
2. nach Erledigung des Auftrags die ihr von der datenverarbeitenden Stelle überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

Die Absätze 1 bis 3 gelten entsprechend.

§ 17
Gemeinsame Verfahren, automatisierte Übermittlungsverfahren

(1) Ein automatisiertes Verfahren, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, darf nur eingeführt werden, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die gesetzlichen Anforderungen an die Zulässigkeit der Datenverarbeitung im Einzelfall bleiben unberührt.

(2) Die beteiligten Stellen haben gemeinsam die Dokumentation gemäß § 5 Absatz 2 Nr. 2 für das gesamte Verfahren aufzustellen. Dabei legen sie über die in dieser Vorschrift genannten Umstände hinaus auch fest

1. den Umfang der Pflichten, die jeder beteiligten Stelle in dem Verfahren zukommen,
2. für jede beteiligte Stelle den Bereich der Datenverarbeitung, für dessen Rechtmäßigkeit sie verantwortlich ist.

Die für das Verfahrensverzeichnis nach § 8 erforderlichen Angaben zu dem gemeinsamen Verfahren einschließlich der Informationen nach Satz 2 werden in die Verfahrensverzeichnisse aller beteiligten Stellen aufgenommen.

(3) Die Freigabe nach § 5 wird von den Leiterinnen oder Leitern der beteiligten Stellen gemeinsam erteilt. Ist den beteiligten Stellen dieselbe Stelle übergeordnet, so erteilt die Leiterin oder der Leiter dieser Stelle die Freigabe.

(4) Die Betroffenen können die ihnen nach dem § 25 Absatz 1 Nummern 1 bis 6 zustehenden Rechte gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Datenverarbeitung verantwortlich ist. Die beteiligten Stellen leiten die Anliegen der Betroffenen an die zuständige Stelle weiter. Der Umfang der Auskunft nach § 27 erstreckt sich auch auf die Angaben nach Absatz 2 Satz 2.

(5) Die Absätze 1 bis 4 gelten entsprechend für automatisierte Verfahren, die eine Übermittlung personenbezogener Daten ohne vorherige Prüfung des Einzelfalles durch die übermittelnde Stelle ermöglichen (automatisierte Übermittlungsverfahren). Absatz 1, Absatz 2 Satz 1 und 2 und Absatz 3 Satz 1 gelten entsprechend, wenn innerhalb einer datenverarbeitenden Stelle ein gemeinsames automatisiertes Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

§ 18
Mobile personenbezogene Datenverarbeitungssysteme

(1) Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme, z. B. Chipkarten), dürfen nur mit der Einwilligung der oder des Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden.

(2) Für die Betroffenen muß jederzeit erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlaßt stattfinden,
2. welche personenbezogenen Daten der oder des Betroffenen verarbeitet werden und
3. welcher Verarbeitungsvorgang im einzelnen abläuft oder angestoßen wird.

Den Betroffenen müssen die Informationen nach Nummer 2 und 3 auf ihren Wunsch auch schriftlich in Papierform mitgeteilt werden.

(3) Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach § 25 zustehenden Rechte aufzuklären. Sofern zur Wahrnehmung der Informationsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür Sorge zu tragen, daß diese in angemessenem Umfang zur Verfügung stehen.

§ 19
Verbot automatisierter Einzelentscheidungen

Entscheidungen, die zu einer tatsächlichen oder rechtlichen Beschwerde der Betroffenen führen, dürfen nicht ausschließlich auf die Ergebnisse automatisierter Verfahren, die einzelne Aspekte der Person der Betroffenen bewerten, gestützt werden. Ergebnisse automatisierter Verfahren dürfen abweichend von Satz 1 für Entscheidungen verwendet werden, wenn

1. ein Gesetz, das angemessene Garantien zur Wahrung der Rechte der Betroffenen enthält, dies vorsieht oder
2. der oder dem Betroffenen vor der Entscheidung ermöglicht wird, ihre oder seine besonderen persönlichen Interessen geltend zu machen.

§ 20
Video-Überwachung und -Aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Video-Überwachung), soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

(2) Das Bildmaterial darf gespeichert werden (Video-Aufzeichnung), wenn die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, sie dokumentieren Vorkommnisse, zu deren Aufklärung die weitere Speicherung erforderlich ist.

§ 21
Fernmessen und Fernwirken

(1) Die Einrichtung von Fernmeß- und Fernwirkdiensten ist nur mit der Einwilligung der oder des Betroffenen zulässig. Die oder der Betroffene muß erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist. Die Einwilligung kann jederzeit widerrufen werden, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses dürfen nicht von der Einwilligung der oder des Betroffenen nach Absatz 1 abhängig gemacht werden. Verweigert oder widerruft die oder der Betroffene ihre oder seine Einwilligung, so dürfen ihr oder ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

Abschnitt V
Besondere Zwecke der Datenverarbeitung

§ 22
Datenverarbeitung für wissenschaftliche Zwecke

(1) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken durch öffentliche Stellen und die Übermittlung personenbezogener Daten durch öffentliche Stellen an Dritte, die die Daten zu wissenschaftlichen Zwecken nutzen wollen, soll in anonymisierter Form erfolgen.

(2) Öffentliche Stellen dürfen personenbezogene Daten zu wissenschaftlichen Zwecken verarbeiten oder an Dritte, die die Daten zu wissenschaftlichen Zwecken nutzen wollen, übermitteln, wenn die Daten pseudonymisiert werden und der mit der Forschung befaßte Personenkreis oder bei Übermittlungen die empfangende Stelle keinen Zugriff auf die Zuordnungsfunktion hat. Steht zur Erfassung der Daten, zur Pseudonymisierung oder Anonymisierung bei der übermittelnden Stelle nicht ausreichend Personal zur Verfügung, so

können die mit der Forschung befaßten Personen diese Aufgaben wahrnehmen, wenn sie zuvor nach dem Verpflichtungsgesetz zur Verschwiegenheit verpflichtet worden sind und unter der Aufsicht der übermittelnden Stelle stehen.

(3) Ist eine Anonymisierung oder Pseudonymisierung nicht möglich, so ist die Datenverarbeitung zu wissenschaftlichen Zwecken durch die öffentliche Stelle selbst zulässig, wenn

1. die oder der Betroffene in die Datenverarbeitung eingewilligt hat,
2. es sich nicht um Daten nach § 10 Absatz 4 handelt und schutzwürdige Belange der oder des Betroffenen wegen der Art der Daten oder wegen der Art der Verwendung für das jeweilige Forschungsvorhaben nicht beeinträchtigt sind oder
3. die Einwilligung der oder des Betroffenen nicht eingeholt werden kann und die Genehmigung der für die datenverarbeitende Stelle zuständigen obersten Aufsichtsbehörde vorliegt.

Unter den Voraussetzungen der Nummern 1 und 3 ist auch die Übermittlung personenbezogener Daten an Dritte, die die Daten zu wissenschaftlichen Zwecken nutzen wollen, zulässig.

(4) Die Genehmigung nach Absatz 3 Nr. 3 wird erteilt, wenn das öffentliche Interesse an der Durchführung des jeweiligen Forschungsvorhabens die schutzwürdigen Belange der oder des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Die Genehmigung muß den Forschungszweck, die Art der zu verarbeitenden Daten, den Kreis der Betroffenen sowie bei Übermittlungen den Empfängerkreis bezeichnen und ist der oder dem Landesbeauftragten für den Datenschutz mitzuteilen.

(5) Sobald der Forschungszweck es gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. Im Fall des Absatz 3 Nr. 3 ist dies der obersten Aufsichtsbehörde zu melden. Die nach Absatz 3 Satz 2 übermittelten personenbezogenen Daten dürfen für einen anderen als den ursprünglichen Forschungszweck nur nach Maßgabe der Absätze 1 bis 3 weiterverarbeitet werden.

(6) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. die oder der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerläßlich ist.

(7) Die übermittelnde Stelle hat empfangende Stellen, auf die dieses Gesetz keine Anwendung findet, zu verpflichten, die Vorschriften der Absätze 5 und 6 einzuhalten und jederzeit Kontrollen durch die oder den Landesbeauftragten für den Datenschutz zu ermöglichen.

§ 23
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Öffentliche Stellen dürfen Daten der Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifrechtlicher Regelungen nur nach Maßgabe der Vorschriften des Landesbeamtengesetzes zu Personalakten verarbeiten.

(2) Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 6 und 7 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 24
Besondere Dokumentationsstelle für Sekten

[*Dieser Paragraph ist nach unserer Auffassung im LDSG entbehrlich.*]

Abschnitt VI
Rechte der Betroffenen

§ 25
Rechte der Betroffenen

(1) Betroffene haben nach Maßgabe dieses Gesetzes ein Recht auf

1. Einsicht in das Verfahrensverzeichnis (§ 8 Abs. 3 und 4),
2. Benachrichtigung bei der Erhebung, Speicherung oder Übermittlung der zu ihrer Person gespeicherten Daten (§ 26),
3. Auskunft über die zu ihrer Person gespeicherten Daten (§ 27),
4. Berichtigung, Sperrung oder Löschung der zu ihrer Person gespeicherten Daten (§ 28),
5. Einwand gegen die Datenverarbeitung aus

besonderen persönlichen Gründen (§ 29),

6. Schadensersatz (§ 30) und
7. Anrufung der oder des Landesbeauftragten für den Datenschutz (§ 32 Absatz 3).

(2) Die in Absatz 1 genannten Rechte der Betroffenen können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

§ 26
Aufklärung, Benachrichtigung

(1) Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise aufzuklären über

1. die Anschrift der datenverarbeitenden Stelle,
2. den Zweck der Datenerhebung,
3. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der Datenverarbeitung,
4. die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind,
5. ihre Rechte nach § 25,
6. den Empfängerkreis bei beabsichtigten Übermittlungen sowie
7. die Auftragnehmenden bei beabsichtigter Datenverarbeitung im Auftrag.

(2) Werden die Daten ohne Kenntnis der Betroffenen erhoben, so sind diese in angemessener Weise über die verarbeiteten Daten und über die in Absatz 1 Satz 1 Nummern 1 bis 3 und 5 bis 7 genannten Umstände zu unterrichten. Sollen die Daten übermittelt werden, so hat die Benachrichtigung spätestens zeitgleich mit der Übermittlung zu erfolgen. Satz 1 und 2 finden keine Anwendung, wenn die Betroffenen auf andere Weise Kenntnis von der Verarbeitung ihrer Daten erlangt haben.

§ 27
Auskunft an Betroffene

(1) Den Betroffenen ist von der datenverarbeitenden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten und den Empfängerkreis von Übermittlungen,
4. die Auftragnehmenden bei Datenverarbeitung im Auftrag sowie
5. die Funktionsweise von automatisierten Verfahren.

Die Betroffenen sollen die Art der personenbezogenen Daten, über die Auskunft verlangt wird, näher bezeichnen.

(2) Den Betroffenen ist nach ihrer Wahl statt der Auskunft die Einsicht in die zu ihrer Person gespeicherten Daten zu gewähren. Die Einsicht wird nicht gewährt, soweit diese mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Die Einsicht erstreckt sich nicht auf Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(3) Die Auskunftserteilung oder die Gewährung von Einsicht unterbleibt, soweit eine Prüfung ergibt, daß

1. dadurch die Erfüllung der Aufgaben der datenverarbeitenden Stelle, einer übermittelnden Stelle oder einer empfangenden Stelle gefährdet würde,
2. dadurch die öffentliche Sicherheit gefährdet oder sonst dem Wohle des Bundes oder eines Landes schwere Nachteile entstehen würden oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) In den Fällen des Absatzes 3 sind die Betroffenen unter Mitteilung der wesentlichen Gründe für die Auskunftsverweigerung darauf hinzuweisen, daß sie sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz wenden können. Eine Begründung erfolgt nicht, soweit dadurch der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die Gründe für die Entscheidung nach Satz 2 sind aufzuzeichnen.

§ 28
Berichtigung, Löschung, Sperrung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Die datenverarbeitende Stelle legt in allgemeinen Regelungen über die Aufbewahrung von Daten den Zeitraum fest, innerhalb dessen die Daten als zur Aufgabenerfüllung erforderlich gelten. Sind personenbezogene Daten in Akten untrennbar im Sinn von § 10 Absatz 5 Satz 2 gespeichert, ist die Löschung nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit von der oder dem Betroffenen bestritten wird und sich weder Richtigkeit noch die Unrichtigkeit nachweisen läßt;
2. sie zur Aufgabenerfüllung nicht mehr erforderlich sind, Rechtsvorschriften jedoch die weitere Aufbewahrung anordnen,
3. die oder der Betroffene anstelle der Löschung die Sperrung verlangt,
4. die Löschung die Betroffene oder den Betroffenen in der Verfolgung ihrer oder seiner Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde,
5. ein Fall von Absatz 2 Satz 3 vorliegt oder
6. bei automatisierten Verfahren die Freigabe nach § 5 nicht vorliegt.

(4) Gesperrte Daten dürfen über die Speicherung hinaus ohne Einwilligung der oder des Betroffenen nicht mehr weiterverarbeitet werden, es sei denn, daß Rechtsvorschriften die Verarbeitung zulassen oder die Nutzung durch die datenverarbeitende Stelle zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder von Dritten liegenden Gründen unerläßlich ist. Die Gründe für die Nutzung gesperrter Daten sind zu dokumentieren. Die datenverarbeitenden Stellen haben durch technische oder organisatorische Maßnahmen sicherzustellen, daß die gesperrten Daten nur nach Maßgabe der Sätze 1 und 2 verarbeitet werden.

(5) Von der Berichtigung, Sperrung oder Löschung nach Absatz 1 Nr. 1 sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt werden.

§ 29
Einwand gegen die Verarbeitung

Die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Der Einwand ist begründet, wenn ein besonderes persönliches Interesse der oder des Betroffenen das öffentliche Interesse an der Verarbeitung der Daten im Einzelfall überwiegt. In diesem Fall ist die Datenverarbeitung insgesamt oder in bestimmten Formen unzulässig.

§ 30
Schadensersatz

(1) Entsteht der oder dem Betroffenen durch eine unzulässige oder unrichtige Verarbeitung ihrer oder seiner personenbezogenen Daten in einem automatisierten Verfahren ein Schaden, so ist ihr oder ihm der Träger jeder öffentlichen Stelle, die diese Daten für sich selbst verarbeitet oder verarbeiten läßt, unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) In Fällen einer schweren Verletzung des Persönlichkeitsrechts kann die oder der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(3) Die ersatzpflichtige Stelle haftet jeder oder jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 250 000 Deutsche Mark. Mehrere Ersatzpflichtige haften gesamtschuldnerisch.

(4) Ist streitig, ob ein Schaden ursächliche Folge einer unzulässigen oder unrichtigen Verarbeitung der Daten in einem automatisierten Verfahren ist, so trifft die Beweislast die datenverarbeitende Stelle.

(5) Auf das Mitverschulden der oder des Betroffenen und die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3 und § 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(6) Die Geltendmachung weitergehender Schadensersatzansprüche aufgrund anderer Vorschriften bleibt unberührt.

Abschnitt VII
Die oder der Landesbeauftragte für den Datenschutz

Die Vorschriften dieses Abschnitts sollen die Modalitäten bei der Bestellung der oder des Landesbeauftragten für den Datenschutz, ihre oder seine Rechtsstellung und die von ihr oder ihm wahrzunehmenden Aufgaben regeln. Im Hinblick auf den im Innenministerium geplanten Entwurf eines Gesetzes zur Neuorganisation des Datenschutzes in Schleswig-Holstein sind die folgenden Vorschriften als vorläufig zu betrachten; der Text muß noch mit dem Vorschlag des Innenministeriums abgestimmt werden. Daher greift dieser Entwurf zunächst auf die bisher geltenden Vorschriften zur Wahl und zur Rechtsstellung der oder des Landesbeauftragten für den Datenschutz zurück. Von materieller Bedeutung sind allerdings die Regelungen in diesem Abschnitt, die der oder dem Landesbeauftragten bestimmte, z. T. neue Aufgaben zuweisen. Diese Normen sind aus der Sicht des Landesbeauftragten unbedingt in ein geändertes LDSG aufzunehmen.

§ 31
Berufung und Rechtsstellung

(1) Das Amt der oder des Landesbeauftragten für den Datenschutz wird bei der Präsidentin oder dem Präsidenten des Schleswig-Holsteinischen Landtages eingerichtet.

(2) Der Landtag wählt ohne Aussprache die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von sechs Jahren. Die Wiederwahl ist nur einmal zulässig. Vorschlagsberechtigt sind die Fraktionen des Schleswig-Holsteinischen Landtages. Kommt vor Ablauf der Amtszeit eine Neuwahl nicht zustande, führt die oder der Landesbeauftragte für den Datenschutz das Amt bis zur Neuwahl weiter.

(3) Die Präsidentin oder der Präsident des Schleswig-Holsteinischen Landtages ernennt die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zur Beamtin oder zum Beamten auf Zeit.

(4) Die oder der Landesbeauftragte für den Datenschutz bestellt eine Mitarbeiterin zur Stellvertreterin oder einen Mitarbeiter zum Stellvertreter. Die Stellvertreterin oder der Stellvertreter führt die Geschäfte, wenn die oder der Landesbeauftragte für den Datenschutz an der Ausübung des Amtes verhindert ist.

(5) Vor Ablauf der Amtszeit kann die oder der Landesbeauftragte für den Datenschutz nur mit einer Mehrheit von zwei Dritteln der Mitglieder des Landtages abberufen werden. Die oder der Landesbeauftragte für den Datenschutz kann jederzeit die Entlassung verlangen.

(6) Die oder der Landesbeauftragte für den Datenschutz ist in der Ausübung des Amtes unabhängig und nur dem Gesetz unterworfen. Sie oder er untersteht der Dienstaufsicht der Präsidentin oder des Präsidenten des Schleswig-Holsteinischen Landtages. Für die Erfüllung der Aufgabe ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen; die Mittel sind im Einzelplan des Landtages in einem gesonderten Kapitel auszuweisen.

(7) Die Mitarbeiterinnen und Mitarbeiter werden auf Vorschlag der oder des Landesbeauftragten für den Datenschutz ernannt. Sie können nur im Einvernehmen mit ihr oder ihm versetzt oder abgeordnet werden. Ihre Dienstvorgesetzte oder ihr Dienstvorgesetzter ist die oder der Landesbeauftragte für den Datenschutz, an deren oder dessen Weisungen sie ausschließlich gebunden sind.

(8) Die oder der Landesbeauftragte für den Datenschutz ist oberste Dienstbehörde im Sinne von § 96 Strafprozeßordnung. Sie oder er trifft die Entscheidungen über Aussagegenehmigungen für sich und die Mitarbeiterinnen und Mitarbeiter in eigener Verantwortung.

§ 32
Kontrollaufgaben

(1) Die oder der Landesbeauftragte für den Datenschutz überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen, auf die dieses Gesetz Anwendung findet. Die Gerichte und der Landesrechnungshof unterliegen der Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

(2) Auf Anforderung des Landtages, des Eingabenausschusses des Landtages oder einer obersten Landesbehörde soll die oder der Landesbeauftragte für den Datenschutz ferner Hinweisen auf Angelegenheiten und Vorgänge, die ihren oder seinen Aufgabenbereich unmittelbar betreffen, nachgehen. Sie oder er legt dem Landtag jährlich einen Tätigkeitsbericht vor.

(3) Jede oder jeder hat das Recht, sich unmittelbar an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz zu wenden, wenn sie oder er annimmt, daß bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen datenschutzrechtliche Vorschriften verletzt wurden. Dies gilt auch für Beschäftigte der öffentlichen Stellen, ohne daß der Dienstweg einzuhalten ist.

(4) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und ihre oder seine Mitarbeiterinnen und Mitarbeiter bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft auf ihre Fragen zu erteilen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme; besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen,
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

Die oder der Landesbeauftragte für den Datenschutz darf im Rahmen von Kontrollen personenbezogene Daten auch ohne Kenntnis der Betroffenen erheben. Die Benachrichtigung der Betroffenen richtet sich nach § 33 Absatz 4.

(5) Stellt die jeweils zuständige oberste Landesbehörde im Einzelfall fest, daß durch eine mit der Einsicht verbundene Bekanntgabe personenbezogener Daten die Sicherheit des Bundes oder eines Landes gefährdet wird, dürfen die Rechte nach Absatz 1 nur von der oder dem Landesbeauftragten für den Datenschutz persönlich oder den von ihr oder ihm schriftlich besonders damit betrauten Beauftragten ausgeübt werden.

§ 33
Beanstandungen

(1) Stellt die oder der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bei öffentlichen Stellen fest, so fordert sie oder er diese zur Mängelbeseitigung auf.

(2) Bei erheblichen Verstößen oder sonstigen erheblichen Mängeln spricht die oder der Landesbeauftragte für den Datenschutz gegenüber der öffentlichen Stelle eine förmliche Beanstandung aus. Sie oder er kann die öffentliche Stelle zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auffordern und die zuständige Aufsichtsbehörde über die Beanstandung unterrichten.

(3) Mit der Feststellung von Mängeln und der Beanstandung sollen Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

(4) Die Betroffenen können mit Kenntnis der datenverarbeitenden Stelle nach pflichtgemäßem Ermessen von Verstößen gegen die Vorschriften dieses Gesetzes oder andere Datenschutzvorschriften unterrichtet werden.

§ 34
Serviceaufgaben

(1) Die oder der Landesbeauftragte für den Datenschutz berät die öffentlichen Stellen in Fragen des Datenschutzes, der Informationssicherheit und der damit zusammenhängenden Datenverarbeitungstechniken sowie deren Sozialverträglichkeit. Zu diesem Zweck können Empfehlungen zur Verbesserung des Datenschutzes gegeben werden. Auf Anforderung des Landtages, einzelner Fraktionen des Landtages oder der Landesregierung hat die oder der Landesbeauftragte für den Datenschutz Gutachten zu erstellen und Berichte zu erstatten.

(2) Die oder der Landesbeauftragte für den Datenschutz berät und informiert die Bürgerinnen und Bürger über alle Fragen des Datenschutzes und der Informationssicherheit, insbesondere über die ihnen bei der Verarbeitung ihrer Daten zustehenden Rechte sowie über geeignete technische Maßnahmen zum Selbstdatenschutz.

(3) Datenverarbeitende Stellen können ihr Datenschutzkonzept durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz prüfen und beurteilen lassen. Das Nähere regelt die Verordnung nach § 5 Absatz 4.

(4) Die oder der Landesbeauftragte für den Datenschutz führt Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durch. Sie oder er berät nichtöffentliche Stellen auf Anfrage in Fragen von Datenschutz und Datensicherheit.

(5) Die oder der Landesbeauftragte für den Datenschutz kann für die Wahrnehmung der Aufgaben nach den Absätzen 3 und 4 Entgelte erheben. Das Nähere darüber regelt die Verordnung nach § 5 Absatz 4.

Abschnitt VIII
Übergangs- und Schlußvorschriften

§ 35
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlaßt.

Ordnungswidrig handelt auch, wer anonymisierte oder pseudonymisierte Daten mit anderen Informationen zusammenführt und dadurch die Betroffene oder den Betroffenen wieder bestimmbar macht oder wer sich bei pseudonymisierten Daten entgegen den Vorschriften dieses Gesetzes Zugriff auf die Zuordnungsfunktion verschafft.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 100 000 Deutsche Mark geahndet werden.

§ 36
Übergangsvorschriften

Soweit andere landesrechtliche Vorschriften den Dateibegriff verwenden, ist Datei

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder
2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nichtautomatisierte Datei).

§ 37
Inkrafttreten

(1) Dieses Gesetz tritt am 1. Januar 2000 in Kraft.

(2) Mit dem Inkrafttreten dieses Gesetzes tritt das Gesetz zum Schutz personenbezogener Informationen vom 30. Oktober 1991 (GVOBl. Schl.-H. S. 555), zuletzt geändert durch Gesetz vom 12. März 1996 (GVOBl. Schl.-H. S. 291), außer Kraft.

Der vollständige Text des Gesetzentwurfes mit Gesetzesbegründung und weiteren Materialien ist als Landtagsdrucksache 14/1738 erschienen und kann beim



Landesbeauftragten für den Datenschutz
Düsternbrooker Weg 82, 24105 Kiel
Telefon: 0431/988-1208, Telefax: 0431/988-1223
E-Mail: LDSH@netzservice.de
Homepage: www.schleswig-holstein.datenschutz.de

kostenlos angefordert werden.

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
Homepage: 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 Urlaub/Dienst-/Arbeitsbefreiung Zeitwertkarten
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 Datenschutz im Justizbereich
Referat LD 2	
Christine Nordmann App. 1216	
Jürgen von der Ohe App. 1206	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Kommunal-, Gewerbe-, Bau-, Wirtschafts- und Personenstandswesen
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 und Beratung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind Mitwirkung bei der Erstellung von Gutachten
Gebhard Uehlken App. 1229	

Referat LD 4	
Dr. Thilo Weichert	Datenschutz im Ausländerbereich
App. 1205	Datenschutz im Bereich der Parlamentsverwaltung
Torsten Koop	Datenschutz im Sozial- und medizinischen Bereich
App. 1218	
Referat LD 5	
Dr. Susanne Rublack	Datenschutz im Polizei- und Verfassungsschutzbereich
App. 1204	Internationales Datenschutzrecht
N.N.	
App.	
Silke Molt	
App. 1203	
Referat LD 6	
Marit Köhntopp	Grundsatzfragen der Neuen Medien und
App. 1214	Informationstechnologien
	Kryptographie
	Technikfolgenabschätzung
Jan Ziegler	EDV-Einsatz der Dienststelle
App. 1213	Anbindung der Dienststelle an das Internet und an andere Netze
	Führung und Veröffentlichung der Dateienübersicht (§ 24 LDSG)
Frank Möller	
App. 1228	
Ingo Ruhmann	Betreuung des Projekts BioTrusT unter den Aspekten des
App. 1217	Datenschutzes
N.N.	Betreuung des Projekts anonymer und unbeobachteter
App. 1228	Internet-Zugang unter Aspekten des Datenschutzes