SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 14/600**
14. Wahlperiode 12. 03. 97

Bericht

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

Neunzehnter Tätigkeitsbericht
(Berichtszeitraum: März 1996 bis März 1997)

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

Dr. Helmut Bäumler

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

Inhaltsverzeichnis **Seite**

1. Zur Situation des Datenschutzes in Schleswig-Holstein

1.1 Beratung ist notwendig, Kontrolle gleichwohl unverzichtbar

Es ist ein gutes Zeichen, daß so viele Behörden von sich aus an der Einhaltung des Datenschutzes interessiert sind und in steigendem Maße die Beratung der Dienststelle in Anspruch nehmen. Auch uns ist es lieber, wenn wir dazu beitragen können, **Fehlentwicklungen von vornherein zu vermeiden**, statt sie erst im Wege der Kontrolle und Beanstandung aufzugreifen. Vielen Behörden ist klar geworden, daß die Ansprüche an das technische Know-how und an die Kenntnis der einschlägigen Gesetzesbestimmungen bei der Konzeption neuer Verfahren so hoch sind, daß man dafür besser eine fachliche Beratung sucht, so wie man in bestimmten Fällen einen Architekten, Steuerberater oder einen Anwalt braucht.

Wir haben also einen erheblichen Teil unserer Kapazität in **Beratungsdienstleistungen** gesteckt. Die Bandbreite reicht von den Fortbildungsangeboten der DATENSCHUTZAKADEMIE bis zur Mitarbeit in Projektgruppen und bei der Vorbereitung einzelner neuer Automationsvorhaben. Dabei legen wir unser Hauptaugenmerk darauf, daß zunächst klar definiert wird, welchem konkreten Zweck ein Verarbeitungsverfahren dienen soll, daß erst dann die technischen Komponenten festgelegt werden und daß schließlich die Anforderungen der Datenschutzverordnung (Dokumentation des Verfahrens, Test und Freigabe sowie Sicherheitskonzepte) beachtet werden.

Was dies mit Datenschutz zu tun hat? Eine wirksame Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere des Erforderlichkeits- und des Zweckbindungsgrundsatzes setzt voraus, daß ein am Gesetz orientiertes „**Sollkonzept**“ des Technikeinsatzes vorliegt. Wer umgekehrt verfährt, also zuerst eine technische Infrastruktur aufbaut und dann die zu erledigenden Aufgaben definiert, hat oft alle Hände voll zu tun, die Risiken und Nebenwirkungen auf ein akzeptables Maß zu reduzieren. Es geht dabei z.B. darum zu verhindern, daß

- Betriebssysteme, Protokolle und Datenbestände manipuliert werden können, ohne „Fingerabdrücke“ zu hinterlassen,
- externe Dienstleister wie Softwarehäuser, Systemlieferanten und Wartungsdienste unbeaufsichtigt an den Datenbeständen arbeiten können,
- Mitarbeiter eigene Datenbestände aufbauen, die die Vorgesetzten nicht mehr kontrollieren können,
- auf Einzelplatz-PC selbst einfachste Sicherheitskomponenten fehlen,

- Mitarbeiter Software entwickeln, die nicht dokumentiert und z.B. bei ihrem Ausscheiden nicht mehr handhabbar ist.

Daß last but not least mit einer streng an der Gesetzeslage und den Notwendigkeiten der Aufgabenerfüllung orientierten Technikausstattung auch eine Menge **Geld gespart** werden kann, ist ein durchaus angenehmer Nebeneffekt.

Im Mittelpunkt der Beratung standen im Berichtsjahr

- die Großprojekte der Polizei und Justiz MEGA, MESTA und COMPAS (vgl. Tz. 4.2.4, 4.4.1, 4.4.2),

- die Zusammenlegung der Rechenzentren der Oberfinanzdirektion und der Datenzentrale im Rahmen von PILS (vgl. Tz. 4.10.1),

- der Entwurf des Krebsregistergesetzes und insbesondere der notwendigen Umsetzungskonzepte (vgl. Tz. 4.8.1),

- die neue Konzeption für Test und Freigabe im Kommunalbereich (vgl. Tz. 6.3),

- unzählige Probleme der Kommunen mit dem Aufbau eigener Datenverarbeitungssysteme (vgl. Tz. 6.2).

Schließlich gehört zum Beratungskonzept unserer Dienststelle auch, daß es keine Beanstandungen ohne konkrete Hinweise gibt, wie der Mangel behoben und für die Zukunft vermieden werden kann.

Gleichwohl zeigte sich auch im Berichtsjahr wieder, daß auf **Kontrollen zur Durchsetzung des Datenschutzes** nicht verzichtet werden kann.

- Ein typisches Beispiel ist die Datenverarbeitung der **Polizei**. Dort waren in den vergangenen Jahren nach mehreren Kontrollen und infolge des neuen Landesverwaltungsgesetzes die Datenbestände drastisch reduziert und auf das gesetzlich zulässige Maß zurückgeführt worden. Im Bereich des **polizeilichen Staatsschutzes** allerdings, der bislang noch nicht systematisch geprüft worden war, fanden wir Datensammlungen vor, an denen unsere Beanstandungen und die Änderungen des Polizeirechts mehr oder weniger spurlos vorübergegangen waren. Dies ist gerade im Hinblick auf die Sensibilität der Datenbestände des Staatsschutzes besonders problematisch. Man fragt sich, wieso die notwendigen Korrekturen erst nach unserer Kontrolle, über vier Jahre nach Inkrafttreten des Landesverwaltungsgesetzes, vorgenommen werden (vgl. Tz. 4.2.1).

- Obwohl das **Patientengeheimnis** eines der ältesten Datenschutzrechte ist, zu dessen Einhaltung jeder Arzt schon nach der ärztlichen Berufs-

ordnung verpflichtet ist, konnten wir bei unserer Kontrolle feststellen, daß es in einem Krankenhaus relativ einfach war, an Patientenakten zu gelangen. Erst jetzt wird dort Abhilfe geschaffen (vgl. Tz. 6.6.2).

- **Sozialdaten** gehören zu den besonders schützenswerten Daten. Gleichwohl gelangte der gesamte Datenbestand eines Sozialamtes an ein Servicehaus, weil die Behörde wegen mangelhafter Organisation nicht selbst in der Lage war, einen Fehler im PC zu beheben. Nach unserer Kontrolle sind umfangreiche Maßnahmen zur Abhilfe eingeleitet worden (vgl. Tz. 6.6.1).

- Durch unsere Kontrollen des **Schleswig-Holstein-Netzes** und des Kommunikationsnetzes **IKONET** wurden Sicherheitsmängel sichtbar, an deren Beseitigung jetzt gearbeitet wird (vgl. Tz. 7.8, 7.9).

- Obwohl die gesetzlichen Bestimmungen für die Löschung von Fahrzeughalterdaten eindeutig sind, verwandten **Zulassungsstellen** ein EDV-Verfahren, das diese Löschungsfristen ignoriert. Jetzt müssen die Programme nachgebessert werden (vgl. Tz. 4.6.1).

- Eigentlich leuchtet es ein, daß Ordnungswidrigkeitenverfahren nicht noch jahrzehntelang in einer **Bauakte** aufbewahrt werden dürfen, gerade wenn längst ein neuer Eigentümer das Grundstück besitzt. Erst nach unserer Kontrolle beginnen jetzt die Bauämter, ihre Akten neu zu organisieren (vgl. Tz. 4.1.1).

- Daß ein Briefkasten so gestaltet sein muß, daß man nicht von außen die Post wieder herausangeln kann, sollte nicht streitig sein. Umso mehr wenn es um ein **Sozialamt** geht, bei dem üblicherweise sensible Schreiben eingehen. Ein Petent hatte sich bei der Stadt Kiel vergeblich über einen völlig ungenügenden Briefkasten beschwert. Erst als er den brisanten Inhalt des Briefkastens bei uns ablieferte und wir die Angelegenheit vor Ort überprüften, kam die Verwaltung in Schwung (vgl. Tz. 9.12).

- Wenn gegen einen Mitarbeiter wegen sexueller Belästigung am Arbeitsplatz **Disziplinarermittlungen** geführt werden, versteht es sich von selbst, daß die Unterlagen im Interesse aller Beteiligten vertraulich behandelt werden. Bei unserer Kontrolle entdeckten wir die Daten aber auf einem PC, auf dem sie „vergessen" worden waren (vgl. Tz. 6.6.3).

Diese kleine Aufzählung, die keineswegs abschließend ist, zeigt, daß der Datenschutz bei aller Aufgeschlossenheit vieler Behörden kein Selbstgänger ist. Gerade weil alle Welt nur von Einsparung und Verschlankung redet, droht der Datenschutz der Bürgerinnen und Bürger auf der Strecke zu bleiben, wenn seine Einhaltung nicht regelmäßig überprüft würde.

Mit einem neuen Prüfkonzept haben wir im Berichtsjahr begonnen, unsere knappen Ressourcen möglichst wirkungsvoll einzusetzen: **angekündigte unangekündigte Kontrollen** (AUK). Während wir ansonsten unsere systematischen Kontrollen in der Regel vorher ankündigen, wird bei den AUK wie folgt verfahren: Ca. 50 Behörden erhalten jeweils die Mitteilung, sie müßten innerhalb der nächsten sechs Monate mit einer unangemeldeten Kontrolle rechnen. Aus den 50 werden etwa zehn durch Los bestimmt, die dann tatsächlich unangemeldeten Besuch erhalten. Dabei werden in erster Linie Aspekte der äußeren Datensicherheit und des sorgfältigen Umgangs mit Daten geprüft, also z.B., ob Büros beim Verlassen abgeschlossen werden, ob PC ausgeschaltet werden, wenn sie unkontrolliert sind, ob Akten auf den Fluren oder in offenen Schränken zugänglich sind, aber auch, welche Kopien mehr oder weniger zerrissen in den Papierkorb, z.B. neben dem Kopierer, geworfen werden. Die Ergebnisse werden derzeit ausgewertet und in den nächsten Tätigkeitsbericht aufgenommen.

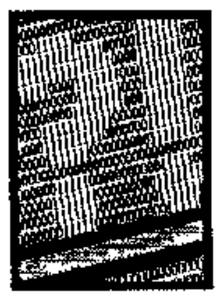
1.2 Die Ausstattung der Dienststelle

Auch im Berichtsjahr hat das Parlament dem Zusammenhang zwischen zunehmender Automatisierung der Datenverarbeitung und der Verstärkung der Datenschutzkontrollen und -beratungen Rechnung getragen. Trotz schwieriger Haushaltslage wurden neue Stellen bewilligt, so daß die Dienststelle nunmehr insgesamt 20 Mitarbeiterinnen und Mitarbeiter umfaßt.

Wir müssen versuchen, mit unseren Mitteln und Ressourcen Schritt zu halten mit den enormen Investitionen des Landes für Informationstechnik in den kommenden Jahren. Deshalb wurde der **technische Anteil** im Personalbereich in den vergangenen Jahren **systematisch ausgebaut**. Von den Mitarbeiterinnen und Mitarbeitern, die unmittelbar für Kontrolle und Beratung eingesetzt werden können, gehört inzwischen nahezu die Hälfte den Technikreferaten an. Durch den Aufbau eines eigenen **IT-Labors** soll dafür Sorge getragen werden, daß diese sich stets mit neuesten Hard- und Softwarekomponenten vertraut machen und so deren Nutzungsmöglichkeiten und die Schwächen beurteilen können.

In zunehmendem Maße beobachten wir die Bestellung **behördlicher Datenschutzbeauftragter**. Die Kreise Pinneberg und Schleswig sind hier mit gutem Beispiel vorangegangen. In anderen Bereichen, z.B. bei den Direktionen der Polizei, stehen Maßnahmen in dieser Richtung offenbar bevor. Gibt man engagierten behördlichen Datenschutzbeauftragten die notwendigen Kompetenzen, Fortbildungs- und Arbeitsmöglichkeiten, so ist dies von Vorteil für **Bürger und Behörden**.

Die meisten behördlichen Datenschutzbeauftragten absolvieren die einschlägigen Kurse der DATENSCHUTZAKADEMIE, die zu einem festen Bestandteil unserer Arbeit geworden ist. Sie finanziert sich nach wie vor nur über die Einnahmen aus den Kursen und verursacht keine Belastung des Landeshaushalts. Die Nachfrage nach den Kursen der DATENSCHUTZAKADEMIE ist ungebrochen, so daß die Beratungstätigkeit der Dienststelle sich nach wie vor auf die Grundlagenarbeit der DATENSCHUTZAKADEMIE stützen kann. Das systematische Zusammenspiel von Kontrolltätigkeit und Beratung im Rahmen der DATENSCHUTZAKADEMIE dokumentieren auch in diesem Bericht die Hinweise auf die einschlägigen Kurse.



1.3 Die Wirkung unserer Arbeit

Datenschutzbeauftragte haben die Aufgabe zu kontrollieren und zu kritisieren, wenn sie Mängel bei der Verarbeitung personenbezogener Daten feststellen. Auch dieser Bericht legt an vielen Stellen den Finger in die Wunde, damit Fehlentwicklungen aufgezeigt und nach Möglichkeit verhindert werden. Auf diese Weise werden aber „Kritik", „Bedenken", „Beanstandung", „gegen" zu häufig gebrauchten Begriffen im Wortschatz der Datenschutzbeauftragten. Bei manchen entsteht daher der Eindruck, sie seien aus Prinzip gegen alles und jedes. Am besten frage man sie nicht, denn sie hätten ohnehin Bedenken.

Die Wirklichkeit sieht, jedenfalls bei uns in Schleswig-Holstein, anders aus. Um einmal deutlich zu machen, wie sich die Arbeit der Datenschutzbeauftragten und insbesondere die konstruktive Zusammenarbeit mit den Behörden konkret für den Grundrechtsschutz der Bürgerinnen und Bürger auswirkt, ist in diesem Bericht erstmals eine Liste enthalten, wofür wir uns **erfolgreich** eingesetzt haben und wo wir - was uns ganz wichtig ist - Konsens mit den Behörden erreicht haben (vgl. Tz. 11.). Sie macht deutlich, daß „der Datenschutz" **nicht** in erster Linie **gegen** etwas ist, **sondern für** konsequente Verbesserungen des **Grundrechtsschutzes** im Interesse der Bürgerinnen und Bürger.

2. Der Weg in die Computergesellschaft

2.1 Der Große Lauschangriff auf leisen Sohlen

Offenbar ist die politische Entscheidung für die Einführung des Großen Lauschangriffs gefallen. Die Polizei soll also das Recht erhalten, für Zwecke der Strafverfolgung auch in Privatwohnungen Abhörmikrofone zu installieren. Aus einem sogenannten „**Eckpunkte-Papier**“ der Bundesministerien des Innern und der Justiz ergeben sich Einzelheiten der geplanten Regelungen. Es bestätigt unsere Befürchtungen gegen den Großen Lauschangriff noch einmal deutlich; denn es sieht keineswegs nur vor, daß sogenannte „Gangsterwohnungen“, wie es immer geheißen hatte, abgehört werden sollen, sondern auch die Wohnungen solcher Personen, die selbst gar nicht verdächtig sind. Außerdem ist offenbar nicht mehr beabsichtigt, in der Verfassung festzulegen, daß der Große Lauschangriff nur zur Aufklärung schwerster Straftaten eingesetzt werden darf. Dadurch wäre ständigen Erweiterungen des Straftatenkatalogs durch den Gesetzgeber mit einfacher Mehrheit Tür und Tor geöffnet. Schon jetzt werden überdies die nächsten Forderungen auf den Tisch gelegt: Es sollen nicht nur Mikrofone, sondern auch geheime Videokameras in privaten Wohnungen versteckt werden dürfen. Wir haben der Ministerpräsidentin nach Bekanntwerden des Eckpunkte-Papiers erneut unsere Bedenken mitgeteilt und sie gebeten, der Einführung des Großen Lauschangriffs nicht zuzustimmen.

Von großer Bedeutung ist in diesem Zusammenhang auch ein **Urteil des Bundesgerichtshofes**. Dieser hat unlängst entschieden, daß unter bestimmten Voraussetzungen Informationen, die mit Hilfe einer Abhörmaßnahme in einer Wohnung zur Gefahrenabwehr nach Landesrecht gewonnen wurden, auch für die Strafverfolgung verwendet werden dürfen. Würde diese Entscheidung Schule machen, könnten die in den Landespolizeigesetzen enthaltenen, ursprünglich zur Abwehr schwerer Gefahren für Leib und Leben gedachten Abhörbefugnisse zur Einführung des Großen Lauschangriffs ohne Verfassungsänderung umfunktioniert werden. In einigen Ländern sind diese Abhörbefugnisse zur Gefahrenabwehr sogar so weit formuliert, daß sich eine Regelung des Großen Lauschangriffs auf der Grundlage des „Eckpunkte-Papiers“ am Ende einengend auswirken würde.

Zwar hält sich das **schleswig-holsteinische Landesverwaltungsgesetz** hinsichtlich der Abhörbefugnis in Wohnungen eng an die grundgesetzlichen Vorgaben und läßt sie nur zu bei einer gegenwärtigen Gefahr für Leib oder Leben einer Person. Gleichwohl wäre es nicht hinnehmbar, wenn eine verfassungsrechtlich und innenpolitisch so umstrittene Maßnahme wie der Große Lauschangriff praktisch durch das Urteil eines Senats des Bundesgerichtshofes eingeführt würde. Auf diesem Wege würde eine breite parlamentarische und öffentliche Debatte darüber

verhindert, inwieweit die Argumente der Befürworter des Großen Lauschangriffs tragfähig sind. Dabei haben die Untersuchungen des schleswig-holsteinischen Innenministeriums belegt, daß die polizeiliche Kriminalstatistik, deren jährliche Veröffentlichung zumeist das Signal zur Forderung nach neuen Eingriffsbefugnissen für die Polizei ist, wie etwa dem Großen Lauschangriff, in beachtlichem Umfang gefälscht und „nach oben" manipuliert worden war. Daraus sollte der Schluß gezogen werden, daß auf derart unsicheren Grundlagen wichtige Grundrechte nicht eingeschränkt werden dürfen.

2.2 Datenschutz durch Technik

Das Thema der **Sommerakademie 1996** „Datenschutz durch Technik - Technik im Dienste der Grundrechte" war offenbar richtig gewählt. In der Datenschutzdiskussion spielen derzeit Erörterungen über den Einsatz datenschutzgerechter Technik eine wichtige Rolle (vgl. Tz. 7.5). Die **Konferenz der Datenschutzbeauftragten** des Bundes und der Länder hat eine Zwischenbilanz zum Thema „Datenvermeidung durch Technik" verabschiedet und den Arbeitskreis Technik beauftragt, weitere Detailvorschläge zu erarbeiten. Auch die **Europäische Kommission** hat in einem Schreiben an den Vorsitzenden der Datenschutzkonferenz angekündigt, sie wolle in ihr nächstes Rahmenprogramm zur Forschung und Entwicklung neuer Technologien ein spezielles Programm zur Förderung von datenschutzfreundlichen Technologien aufnehmen. Erstmals finden sich auch in den Gesetzentwürfen des Bundes sowie im Mediendienste-Staatsvertrag der Länder Bestimmungen, die die Anbieter verpflichten, die Gestaltung und Auswahl technischer Einrichtungen für Teledienste von vornherein so auszurichten, daß keine oder so wenig wie möglich personenbezogene Daten erhoben, verarbeitet und genutzt werden (vgl. Tz. 7.2).

Es ist jetzt Sache der **Betreiber und Hersteller**, die vielen konstruktiven Vorschläge für mehr Grundrechtsschutz durch Technik aufzunehmen und in die Tat umzusetzen. Daraus werden sich im Ergebnis Wettbewerbsvorteile ergeben, weil die Bürger im Zweifel diejenigen Produkte bevorzugen werden, die mit ihrem Recht auf informationelle Selbstbestimmung am schonendsten umgehen.

2.3 Verschlüsselung: die Chance!

Eine wichtige grundrechtsfreundliche Technik ist die Kryptografie, das heißt die Möglichkeit, Texte so zu verschlüsseln, daß sie mit den heutigen technischen Mitteln kaum zu knacken sind. In einer Zeit, in der immer mehr Bürgerinnen und Bürger weltweit in offenen Netzen kommunizieren, sind wirksame Verschlüsselungsverfahren wie ein **Geschenk des Himmels**. Sie erlauben es, das Recht auf Wahrung der

Vertraulichkeit und Privatsphäre auch in einer prinzipiell offenen, vielerlei Angriffen ausgesetzten technischen Umgebung wirksam zu schützen. Gleichwohl gibt es in Deutschland und in anderen Ländern Überlegungen, die Nutzung von Verschlüsselungsverfahren zu verbieten oder jedenfalls einzuschränken. Die Begründung ähnelt der, die auch für die Einführung des Großen Lauschangriffs verwendet wird: Verschlüsselungsverfahren könnte sich auch die Organisierte Kriminalität zunutze machen. Deshalb müsse man sie verbieten oder nur solche Schlüssel zulassen, die auch Polizei und Geheimdienste entziffern könnten.

Dabei wird übersehen, daß gerade die Gefahren der **Organisierten Kriminalität** dafür sprechen, Verschlüsselungsverfahren zu fördern und nicht etwa zu verbieten. Denn wie sonst sollen sich Wirtschaft und Verbraucher bei finanziellen Transaktionen über offene Netze vor kriminellen Attacken schützen? Wenn der Satz „Prävention geht vor Repression" eine Bedeutung hat, dann hier. Es ist wie mit dem Kfz-Diebstahl: Eine wirksame elektronische Wegfahrsperre ist sinnvoller, als die mühsame polizeiliche Fahndung nach gestohlenen Autos.

Es geht aber auch um folgendes: Bislang gibt es in der deutschen Rechtsordnung keine Vorschrift, die den Bürger verpflichtet, der Polizei vorsorglich seine Geheimnisse anzuvertrauen für den Fall, daß einmal gegen ihn ermittelt werden muß. Niemand muß bei der Polizei seinen Wohnungsschlüssel hinterlegen, damit etwaige Hausdurchsuchungen leichter durchführbar sind oder gar ein Verzeichnis seiner häuslichen Verstecke, damit sie im Falle eines Falles besser gefunden werden können. Bis heute ist es nicht verboten, in Briefen eine Geheimsprache oder auch nur einen seltenen Dialekt zu verwenden, den Polizei und Geheimdienst nicht verstehen. Vielmehr ist es deren Sache, Briefinhalte zu verstehen, wenn sie etwa auf der Grundlage der einschlägigen gesetzlichen Bestimmungen einen Brief geöffnet haben.

Nur weil auch einige Kriminelle die Verschlüsselung für ihre Zwecke nutzen könnten, darf den Bürgern diese hervorragende Möglichkeit, ihre privaten Informationen wirksam vor fremder Neugier zu schützen, nicht vorenthalten werden. Man könnte sonst nämlich den Gedanken fortführen und fragen, ob man nicht Urlaubsreisen verbieten oder einschränken sollte, weil sich bekanntlich immer auch Rauschgiftschmuggler in den Touristenstrom mischen. Oder man könnte Autos verbieten, die schneller als 150 km in der Stunde fahren, damit die Polizei und die Geheimdienste immer bequem hinterherkommen usw.

Es bleibt zu hoffen, daß die Politik die Verschlüsselung als das begreift, was sie ist: eine **einmalige Chance**, die Privatsphäre auch in einer problematischen technischen Umgebung wirksam zu schützen. Im übrigen sind sich die Experten ziemlich einig, daß ein **Verbot** oder eine Einschränkung der Kryptografie **wirkungslos** wäre. Es wäre gerade für die, gegen die es gerichtet wäre, nämlich raffinierte organisierte Krimi-

nelle, leicht zu umgehen. Zum angestrebten Zweck wäre es also völlig ungeeignet. Damit würde eine Reglementierung der Verschlüsselung aber gegen das verfassungsmäßige Verhältnismäßigkeitsprinzip verstoßen, weil es gesetzestreuen Bürgern die Chance zum Schutz ihrer Privatsphäre nehmen würde, ohne daß Rechtsbrecher gehindert wären, solche Verbote nach Belieben zu umgehen (vgl. Tz. 7.6).

3. Datenschutz im Landtag

3.1 Gesetzgebung

Der Landtag hat das schleswig-holsteinische **Krebsregistergesetz** verabschiedet. Es sieht eine Pflicht für alle Ärzte vor, Krebserkrankungen an das Register zu melden. Ist ein Patient damit nicht einverstanden oder kann er nicht um Einwilligung gebeten werden, wird sein Fall anonym gemeldet. Auf diesem Weg soll ein möglichst hoher Prozentsatz an Meldungen erreicht und zugleich das Recht auf informationelle Selbstbestimmung gewahrt werden (zu den Einzelheiten vgl. Tz. 4.8.1). Im Ergebnis ist es gelungen, die Grundlage für ein wissenschaftlich aussagefähiges Register zu schaffen und zugleich die Belastung der Betroffenen durch die Möglichkeit der Anonymisierung gering zu halten. Allerdings ist es nicht ausgeschlossen, daß bei einzelnen Datensätzen auch ein **Risiko der Deanonymisierung** entstehen kann, wenn ein entsprechendes Zusatzwissen vorhanden ist. Die Registerstelle muß gewährleisten, daß bei Bestehen derartiger Risiken auch anonymisierte epidemiologische Daten nicht herausgegeben werden.

Das Gesetz weist auch dem **Landesbeauftragten für den Datenschutz** eine neue Rolle zu: In bestimmten Fällen hat er die Referenzlisten gemeldeter Krebspatienten **treuhänderisch** und sicher zu verwahren. Erstmals hat das Gesetz auch im Datenschutzrecht das **Verursacherprinzip** zur Geltung gebracht. Diejenigen Stellen, die Daten aus dem Krebsregister für Forschungszwecke erhalten, müssen sich der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwerfen. Die Kosten der Kontrolle können durch Gebühren bis zur Höhe von 20.000,- DM auf die geprüfte Stelle umgelegt werden.

Mit dem Innenministerium haben erste Gespräche über ein **Sicherheitsüberprüfungsgesetz** stattgefunden. Hinsichtlich der aufgrund der EU-Datenschutzrichtlinie (vgl. 18. TB, Tz. 1.1.1) bis 01.10.1998 notwendigen Novellierung des **Landesdatenschutzgesetzes** sind noch keine Entwürfe des Parlaments oder der Regierung bekanntgeworden. Umfangreiche Vorüberlegungen für ein neues **Landesmeldegesetz** (vgl. Tz. 4.1.2) sowie für eine Novellierung des **Schulgesetzes** (vgl. Tz. 4.9.1) lassen erwarten, daß in diesen Bereichen die Datenverarbeitung neu geregelt wird.

3.2 Datenschutzordnung

Nachdem wir in früheren Tätigkeitsberichten (vgl. 17. TB, Tz. 3.3, 18. TB, Tz. 3.3) die Notwendigkeit und den Inhalt parlamentarischer Datenschutzregelungen erörtert hatten, wurde das Thema auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

aufgegriffen. Ausgangspunkt waren die Vorarbeiten, die die **Konferenz der Parlamentsdirektoren** geleistet hat.

Es wurde deutlich, daß die **Rechtsgrundlagen** in den Bundesländern **nicht einheitlich** sind. Dennoch zeigen sich einige Gemeinsamkeiten:

- Wenn die Datenschutzregelung Außenwirkungen zugunsten der betroffenen Menschen entfalten soll, ist zumindest eine für Abgeordnete und Fraktionen verbindliche und im Gesetzblatt **veröffentlichte Datenschutzordnung** vonnöten.

- Das **Kontrollverfahren** muß zwar substantielle datenschutzrechtliche Prüfungsmöglichkeiten sicherstellen, aber auch den besonderen verfassungsrechtlichen Status der Abgeordneten, insbesondere die Freiheit des Mandats, berücksichtigen.

- Von der Möglichkeit, im Landtag die personenbezogene Verarbeitung von Informationen, die Abgeordneten ausschließlich **zweckgebunden** und **freiwillig** übermittelt werden, einzuschränken oder auf einen kleineren Kreis von Informationsempfängern zu begrenzen, sollte Gebrauch gemacht werden.

- Bei der Veröffentlichung personenbezogener **Daten der Abgeordneten** können im Einzelfall überwiegende Gesichtspunkte des Persönlichkeitsschutzes Einschränkungen rechtfertigen.

Diese Überlegungen haben auch in den Erörterungen einer Datenschutzordnung für den Schleswig-Holsteinischen Landtag eine wesentliche Rolle gespielt. Die Arbeiten an einem entsprechenden Entwurf sind zu einem vorläufigen Abschluß gekommen. Er wurde mittlerweile dem Parlament zugeleitet und soll zügig beraten werden.

Was ist zu tun?
Die Datenschutzordnung sollte möglichst bald in Kraft treten.

4. Datenschutz in der Verwaltung

4.1 Kommunalbereich

4.1.1 Eine Bauakte für alle Fälle

Die Kontrolle der Datenverarbeitung in einem Bauamt förderte eine Reihe von Mängeln zutage. Es ist zu vermuten, daß auch in anderen schleswig-holsteinischen Bauaufsichtsbehörden Handlungsbedarf besteht.

Die Neufassung der Landesbauordnung war für uns Anlaß, bei einer Stadt das bauaufsichtliche Verfahren einer datenschutzrechtlichen Kontrolle zu unterziehen. Es haben sich eine Reihe von Beanstandungen ergeben:

- **Beteiligung Dritter**

  In Erlaubnisverfahren für gewerblich genutzte Räume wurde das **Gewerbeaufsichtsamt** zur Prüfung arbeitsschutzrechtlicher Belange auch dann beteiligt, wenn in den Antragsunterlagen gar kein Hinweis auf eine Beschäftigung von Arbeitnehmern enthalten war. Die Datenübermittlung war mithin **nicht erforderlich**.

- **Unterrichtung des Finanzamtes über die Fertigstellung baulicher Anlagen**

  Nach Eingang von Baufertigstellungsanzeigen wurde darüber das zuständige **Finanzamt** auf der Grundlage des Bewertungsgesetzes informiert. Allerdings wurde versäumt, die Betroffenen vom Inhalt der Mitteilung zu unterrichten, so wie es das Gesetz vorschreibt.

- **Trennung der bauaufsichtlichen Unterlagen von anderen Verwaltungs- und Sachvorgängen**

  Für jedes bebaute Grundstück wurde eine einzige bauaufsichtliche Verfahrensakte geführt, in der sich z.B. auch folgende Unterlagen befanden:

  - Bußgeldbescheide
  - unbegründete Beschwerden von Nachbarn
  - Haushalts- und Kassenunterlagen über die Finanzierung einer bauaufsichtsbehördlichen Ersatzvornahme
  - Entscheidungen nach der Baumschutzsatzung und der Abwasserbeseitigungssatzung

Aus dem Grundsatz der Zweckbindung folgt, daß in Bauerlaubnisakten nur Unterlagen gespeichert werden dürfen, die zur Dokumentation der bauaufsichtlichen Entscheidungen erforderlich sind. Für die anderen Verwaltungsverfahren sind **gesonderte Akten** anzulegen, damit z.B. unterschiedliche Löschungsfristen beachtet werden können.

- **Trennung der Akten nach unterschiedlichen Beteiligten**

  Unterlagen über baurechtliche Verfahren des Eigentümers wurden mit Unterlagen über die Nutzungsuntersagung gegenüber dem Mieter der Wohnung vermischt. Unterlagen über ein Ordnungswidrigkeitenverfahren gegen den Eigentümer waren z.B. zusammen mit einem Beschluß des Verwaltungsgerichts über die Ablehnung eines Prozeßkostenhilfeantrages des Mieters, einschließlich seiner Erklärung über seine persönlichen und wirtschaftlichen Verhältnisse sowie die seiner Familienangehörigen, in einer Akte abgeheftet.

- **Löschung von Daten aus bauaufsichtlichen Verwaltungsverfahren**

  Die Bauerlaubnisakten wurden prinzipiell dauerhaft aufbewahrt. Erst durch die Trennung der verschiedenen Vorgänge besteht künftig auch die Möglichkeit, Unterlagen, die zur rechtmäßigen Aufgabenerfüllung nicht mehr benötigt werden, **fristgerecht zu vernichten**.

Die geprüfte Stelle hat die Beanstandungen und Anregungen positiv aufgegriffen und in ihrer Stellungnahme ausgeführt: „Die im Prüfungsbericht angesprochenen Beanstandungen hinsichtlich der Beachtung des Landesdatenschutzgesetzes im bauaufsichtlichen Verfahren sind zwischenzeitlich beachtet und abgestellt worden."

Was ist zu tun?
Die schleswig-holsteinischen Bauaufsichtsbehörden sollten die Beanstandungen in diesem Einzelfall zum Anlaß nehmen, ihre eigene Verfahrensweise zu überprüfen und ggf. entsprechend zu ändern.

4.1.2 Neues Melderecht in Vorbereitung

Eine Neufassung des Landesmeldegesetzes soll weitreichende Veränderungen bei der Verarbeitung von Meldedaten bringen. Datenschutzrechtliche Vorschläge wurden bei der Erarbeitung des Gesetzentwurfs größtenteils berücksichtigt. Verbliebene strittige Fragen müssen im Rahmen der weiteren Beratungen geklärt werden.

Durch die Änderung des Melderechtsrahmengesetzes im Jahr 1994 hat sich die Notwendigkeit ergeben, das Landesrecht entsprechend anzupassen. Wir haben deshalb dem Innenministerium in einer Stellungnahme 49

Änderungsvorschläge vorgetragen. Der überwiegende Teil wurde in den Gesetzentwurf aufgenommen. Hervorzuheben sind folgende **Verbesserungen**:

- Es dürfen nicht mehr **alle** früheren Anschriften, sondern nur die jeweils letzte gespeichert werden.

- Bei der Anmeldung müssen die Betroffenen im Sinne des datenschutzrechtlichen Transparenzgebotes über die beabsichtigte Weiterverarbeitung ihrer Daten durch die Meldebehörde **aufgeklärt** werden.

- Die Befugnisgrundlagen für die Verarbeitung von **Hotelmeldescheinen** werden präzisiert. Dies gilt insbesondere für Regelungen über die Einsichtnahme durch und die Übermittlung an Dritte.

- In Fällen, in denen für Betroffene eine **Auskunftssperre** wegen Gefahr für Leib und Leben besteht, sollen auch die Auskunftsmöglichkeiten an andere öffentlichen Stellen beschränkt werden. Ein Abruf entsprechender Daten mit Hilfe automatisierter Übermittlungsverfahren soll ganz ausgeschlossen werden.

- Vor der Erteilung von Melderegisterauskünften soll eine sorgfältige **Identifizierung** der angefragten Person zwingend vorgeschrieben werden. Hierzu ist es erforderlich, daß von der anfragenden Person oder Stelle im Regelfall auch das Geburtsdatum oder eine frühere Anschrift des Betroffenen mitgeteilt wird. Fehlerhafte Auskünfte, über die wir z.B. in unserem 18. Tätigkeitsbericht (vgl. Tz. 4.1.2) berichtet haben, sollen dann nicht mehr vorkommen.

Änderungsbedarf sehen wir noch bei folgenden Regelungen:

- Bezüglich der **Sperrung** von Daten bleibt der Entwurf hinter den allgemeinen datenschutzrechtlichen Standards zurück. So sollen Daten, die vom Betroffenen bestritten wurden, ohne daß sich deren Richtigkeit oder Unrichtigkeit feststellen läßt, nicht besonders gekennzeichnet werden. Selbst eine Übermittlung soll zulässig sein, wenn ein entsprechender Hinweis auf die umstrittene Richtigkeit erfolgt.

- Das Melderecht sieht „in besonderen Fällen" die Erteilung von Melderegisterauskünften ausdrücklich vor. So können politische Parteien vor der Wahl Daten erhalten, Mandatsträger, Presse und Rundfunk über Jubiläumsdaten informiert sowie Adreßbuchverlagen Namen und Anschriften volljähriger Einwohner zur Veröffentlichung in einem Adreßbuch bereitgestellt werden. In allen Fällen besteht für die Betroffenen die Möglichkeit, der Datenübermittlung zu widersprechen. Eine solche **Widerspruchsmöglichkeit** ist aus datenschutzrechtlicher Sicht nur eine Notlösung, da das Schweigen der Betroffenen als Zustim-

mung gewertet wird. Bisher wurde auf das Widerspruchsrecht lediglich bei der Anmeldung oder bei beabsichtigter Weitergabe der Daten an Adreßbuchverlage mit amtlicher Bekanntmachung hingewiesen. Beschwerden haben uns gezeigt, daß dies nicht ausreicht. Es sollte deshalb keinen unverhältnismäßigen Aufwand erfordern, alle Personen, auch wenn sie nicht in jüngster Zeit umgezogen sind, schriftlich auf ihr Widerspruchsrecht hinzuweisen, wenn schon nicht die sauberste Lösung, nämlich die Einwilligung der Betroffenen, durchsetzbar ist.

- Durch eine gesetzliche Regelung soll die Befugnis geschaffen werden, Bürgermeistern amtsangehöriger Gemeinden zur Erfüllung ihrer **Repräsentationspflicht** Daten bei der Anmeldung, der Abmeldung, bei einem Alters- oder Ehejubiläum, bei der Geburt eines Kindes und bei einem Sterbefall zu übermitteln. Die Wahrnehmung solcher Repräsentationsaufgaben sollte jedoch nach unserer Auffassung grundsätzlich im Einvernehmen mit den Betroffenen erfolgen, zumindest sollten diese die Möglichkeit haben, einer Datenübermittlung an ehrenamtliche Bürgermeister zu widersprechen.

4.1.3 CD-ROM nur ein modernes Buch?

Zwischen gedruckten Adreßbüchern und solchen Adreßregistern, die auf einer CD-ROM gespeichert und vielseitig erschließbar sind, bestehen so grundlegende qualitative Unterschiede, daß für letztere eine Meldedatenübermittlung nicht zulässig ist.

Verschiedene Meldebehörden wurden von privaten Firmen um Übermittlung von Einwohnerdaten gebeten. Man berief sich auf das Landesmeldegesetz, das die Übermittlung für die Herausgabe von Adreßbüchern grundsätzlich zuläßt, sofern der Betroffene nicht widersprochen hat. Allerdings - so teilten die Firmen mit - wolle man keine Adreßbücher drucken, sondern eine moderne **„Bürger-Info“** über Namen, Anschriften, Telefon- und Fax-Nummern auf CD-ROM erstellen, die durch Werbeinformationen ergänzt werden solle. Für den einzelnen Einwohner wäre die Information gegen eine „Schutzgebühr“ frei erhältlich. Man verzichte darauf, vorhandene Adreßbücher zu scannen oder von Hand elektronisch zu erfassen, „um die Schutzgebühr für die Bürger der Stadt möglichst gering zu halten“.

Stichwort: CD-ROM
CD-ROM steht für „Compact Disk Read Only Memory“ und bezeichnet ein optisches Speichermedium, das, einmal beschrieben, nur gelesen werden kann. Jede dieser „Silberscheiben“ ist mit einer Oberfläche beschichtet, auf der die Information mittels Laser aufgezeichnet und gelesen wird. Die typische Speicherkapazität einer CD-ROM beträgt 650 MB und bietet damit Platz für etwa 325000 DIN-A4-Textseiten.

Für das Speichermedium „CD-ROM" bestehen Auswertungs- und Verknüpfungsmöglichkeiten weit über die herkömmlichen Adreßbücher hinaus. Sie können nicht mehr nur nach Namen oder nach Anschriften, sondern auch nach Berufen, Geschlecht, Singleeigenschaft und anderen Merkmalen ausgewertet werden. Die Nutzungsmöglichkeit solcher Verzeichnisse und die Verbindung mit weiteren Datenbeständen auf CD, wie Telefonbüchern, gewähren Einblicke in den Einwohnerdatenbestand der Meldeämter, die in ihrem Informationsgehalt mit den Auswertungen konventioneller Adreßbücher nicht mehr vergleichbar sind. Wir sind daher in Übereinstimmung mit dem Innenministerium der Auffassung, daß eine Datenübermittlung für ein **„Adreßbuch" auf CD-ROM unzulässig** ist, weil sie nicht dem Melderecht entspricht, das nur Adreß**bücher** erlaubt.

Was ist zu tun?
Die Übermittlung von Meldedaten für Adreßregister auf CD-ROM hat nach geltendem Recht zu unterbleiben. Eine Lockerung ist nur dann zu vertreten, wenn das Widerspruchsrecht der Betroffenen entscheidend verbessert wird.

4.1.4 Datenschutz im Bürgerbüro

Bestrebungen, den Service der Verwaltung für den Bürger zu verbessern, führen zunehmend zur Bildung zentraler Auskunfts- und Beratungsstellen. Solche Bürgerbüros können sinnvoll sein, müssen aber so organisiert werden, daß der Grundsatz der Zweckbindung nicht gefährdet wird.

Immer mehr Städte und Gemeinden wollen im Rahmen der Verwaltungsreform sogenannte **Bürgerbüros** einführen. Man verspricht sich ein kostengünstigeres Anbieten der Leistungen, eine bürgernähere Verwaltung und sogar einen Zugewinn an Demokratie. Bei manchen Bürgern besteht allerdings die Befürchtung, daß für ihren Datenschutz Risiken entstehen. Insbesondere stellen sie die Frage, ob die **Zweckbindung der Daten** noch gewährleistet ist, wenn sämtliche Angelegenheiten an einer Stelle erledigt werden, wie z. B. An- und Abmeldungen,

Stichwort: Bürgerbüro
„Bürgerbüros" sollen den Kontakt zwischen der öffentlichen Verwaltung, insbesondere der Kommunalverwaltung, mit ihren verschiedenen Bereichen und ihren „Kunden" (Antragstellern, Einwohnern, Bürgern) vereinfachen und erleichtern. Ihre Aufgaben sind nicht abschließend definiert. Sie können sich einerseits auf bloße Wegweiserfunktionen beschränken, also z.B. Antragstellern den zuständigen Gesprächspartner vermitteln; ihnen kann aber z.B. auch die Befugnis übertragen sein, Bürger sachlich zu beraten, ihre Anträge für die verschiedenen Zuständigkeitsbereiche entgegenzunehmen und vorzuprüfen.

die Erstellung von Lohnsteuerkarten, die Erhebung von Gebühren, Steuern und Abgaben sowie die Bearbeitung von Sozialhilfeangelegenheiten. In manchen Eingaben wurde die Gefahr vom „gläsernen Bürger" beschworen.

Im Grunde hat dieses Problem gerade bei kleineren Verwaltungen schon immer bestanden. Dort ist der einzelne Mitarbeiter oft für mehrere Aufgabenbereiche zuständig, in der Verwaltungsspitze laufen alle Informationen zusammen. Vielfach bestehen auch zufällige Kenntnisse aus bloßem Interesse über den eigenen Zuständigkeitsbereich hinaus.

Dem steht die vom Bundesverfassungsgericht geforderte **Zweckbindung** bei der Verarbeitung personenbezogener Daten entgegen. Der Gesetzgeber hat für einige Bereiche besondere Anordnungen getroffen, die die Beachtung des Zweckbindungsgrundsatzes auch organisatorisch sicherstellen sollen. Dies gilt z.B. für die Wahrnehmung von Statistikaufgaben, für die Beihilfegewährung an Mitarbeiter im öffentlichen Dienst sowie im Bereich des Gesundheits-, Steuer- und Sozialwesens. Im übrigen gilt die Rechtsprechung des Bundesverfassungsgerichts, daß Gesetzgeber und Verwaltung **organisatorische Vorkehrungen** gegen mögliche Datenschutzverletzungen zu treffen haben.

In derartigen Bürgerbüros tritt das Problem einer „**Datenvermischung**" natürlich verstärkt auf. Hier besteht außerdem in besonderem Maße die Pflicht zu gewährleisten, daß die Verwendung von Daten nachvollziehbar ist. Der Auskunftsanspruch Betroffener erstreckt sich auch hierauf. Generell muß in **Bürgerbüros** der **gleiche Datenschutzstandard** eingehalten werden wie bei herkömmlicher Verwaltungsorganisation auch. In jedem Falle sollte die Möglichkeit erhalten bleiben, daß sich Bürger, wenn sie dies wünschen, auch weiterhin unmittelbar an die Fachdienststellen wenden können.

Was ist zu tun?

Wer Bürgerbüros einrichten möchte, muß sicherstellen, daß dabei nicht der Datenschutzservice verschlechtert wird.

4.2 Polizei

4.2.1 Prüfung beim Staatsschutz

Schneller als der Polizei erlaubt speicherte der Staatsschutz personenbezogene Daten. Nach einer datenschutzrechtlichen Querschnittsprüfung sind umfangreiche Bereinigungsaktionen im Gange.

Eine systematische Kontrolle im Dezernat für Staatsschutzdelikte des Landeskriminalamtes (LKA) hat gezeigt, daß es in diesem Bereich polizeilicher Datenverarbeitung noch **erhebliche Umsetzungsdefizite** des 1992 neugefaßten Landesverwaltungsgesetzes (LVwG) gibt. So kam stellenweise eine Auslegung der Vorschriften zutage, die sich weder mit dem Wortlaut der Normen noch mit dem Willen des Gesetzgebers in Einklang bringen läßt. Anders als der Verfassungsschutz nach dem Landesverfassungsschutzgesetz besitzt der polizeiliche Staatsschutz **keine Vorfeldkompetenz** zur Beobachtung politisch motivierter Gruppierungen oder Bestrebungen, die sich gegen die freiheitlich demokratische Grundordnung oder die Sicherheit des Bundes oder eines Landes richten. Seine Aufgabe ist dieselbe wie die der übrigen Polizei: Straftaten aufklären und konkrete Gefahren abwehren.

Stichwort: Polizeilicher Staatsschutz
Sammelbegriff der für die Verfolgung von Staatsschutzdelikten zuständigen Polizeidienststellen. Unter dem Begriff „Staatsschutzdelikte" werden die Straftaten zusammengefaßt, die gegen die Existenz des Staates, seine verfassungsmäßige Ordnung, seinen gebietsmäßigen Bestand oder seine Sicherheit gerichtet sind.

Wir haben deshalb eine Reihe von Beanstandungen ausgesprochen und auf die strikte **Aufgabentrennung** zwischen **Polizei** und **Verfassungsschutz** hingewiesen. Im einzelnen war folgendes zu kritisieren:

- **Personenakten und Kartei „Innere Sicherheit"**

  Im Bereich „Innere Sicherheit" werden Informationen über **Staatsschutzdelikte** in Personenakten und in der dazugehörigen Kartei „Innere Sicherheit" gespeichert. Für die Einordnung als ein Staatsschutzdelikt reicht der politische Bezug einer Straftat allein noch nicht aus. Vielmehr setzt dies ein besonderes Gewicht der Tat und eine Gefährdung von Rechtsgütern der freiheitlich demokratischen Grundordnung voraus.

  Auch für diese Datenbestände müssen die Regelungen, wie sie im Landesverwaltungsgesetz (§ 189), in den KpS-Richtlinien und in der KA-Regelung festgeschrieben sind, Anwendung finden. Dementsprechend dürfen sie nur die für eine Prognose übet die Wahrscheinlichkeit künftiger Straftaten wesentlichen Informationen enthalten. Die

von uns geprüften 56 Personenakten standen fast durchgehend nicht im Einklang mit diesen Anforderungen.

Beispiele:

- Eine Gruppe von zehn Jugendlichen stieß vor einer Kneipe zwei Blumenkübel um. Einer der Jugendlichen soll „Sieg Heil" gerufen haben, wer, ließ sich aus dem dazugehörigen Vorgang nicht feststellen. Dennoch wurden zu allen zehn Jugendlichen Personenakten angelegt. Die Namen und ein Vermerk über den Vorfall wurden an die Landesverfassungsschutzbehörde und das Bundeskriminalamt übermittelt.

- Im Frühjahr 1995 kam es in Westerland/Sylt zu sogenannten „Chaos-Tagen", bei denen eine mit der Bahn angereiste Menge erhebliche Sachbeschädigungen begangen hat. 99 Personen wurden erkennungsdienstlich behandelt. Die Unterlagen wurden nach der Einstellung des Verfahrens vernichtet. In dem dazugehörigen Ermittlungsvorgang findet sich folgender Vermerk des LKA: „ ... Der Tatverdacht des Landfriedensbruchs konnte gegen keinen der Verdächtigen aufrechterhalten werden." Dennoch wurden sämtliche aus Schleswig-Holstein stammenden Teilnehmer mit dem Vorwurf des Landfriedensbruchs (zumeist erstmalig) gespeichert.

Stichwort: KpS-Richtlinien und KA-Regelung

Die „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen" (KpS-Richtlinien) regeln auf der Grundlage von LDSG und LVwG die Verarbeitung personenbezogener Daten in besonders verfügbaren Datensammlungen, die von der Polizei zur Unterstützung bei der Erfüllung ihrer Aufgaben auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung geführt werden.

Während sich die KpS-Richtlinien auf sämtliche Datensammlungen beziehen, beschränkt sich die „Regelung für das Anlegen und Führen von Kriminalakten" (KA-Regelung) auf Vorgaben für die Führung der klassischen Kriminalakten.

- Im Rahmen eines Ermittlungsverfahrens wegen Verstoßes gegen das Versammlungsgesetz hat ein Polizeipräsidium eines anderen Bundeslandes eine umfangreiche Auflistung mit den Personalien von ca. 250 Personen übersandt. Dies war verbunden mit der Bitte, soweit Zuständigkeit bestehe, die angegebenen Wohnadressen zu überprüfen und ggf. eigene Erkenntnisse zu diesen Personen zu übermitteln. Zu neun Personen aus Schleswig-Holstein wurden aufgrund dieser Anfrage Personenakten angelegt, obwohl weitere Erkenntnisse nicht vorlagen.

Zu diesen Beispielen ist anzumerken: Speicherungen zu einer Person sind nur dann zulässig, wenn sich ein tatsächlicher Verdacht ihrer strafrechtlichen Beteiligung ergibt (vgl. § 189 LVwG). Bei Verfahrenseinstellungen ist eine Weiterspeicherung auf präventiver Grundlage nur möglich, wenn konkrete Anhaltspunkte für eine Täterschaft durch die Unterlagen des Gerichts, der Staatsanwaltschaft oder der Polizei belegt sind. Dies war den geprüften Akten nicht zu entnehmen.

Im Wortlaut: § 189 Abs. 1 LVwG
Die Polizei kann personenbezogene Daten, die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die einer Straftat verdächtig sind, speichern, verändern und nutzen, wenn wegen der Art oder Ausführung und Schwere der Tat sowie der Persönlichkeit der oder des Verdächtigen die Gefahr der Wiederholung besteht und wenn dies zur Aufklärung oder Verhütung einer künftigen Straftat erforderlich ist.

- **Datenspeicherungen wegen vermuteter künftiger Straftaten**

  Hierbei geht es um die Möglichkeit, wegen eines **vermuteten künftigen Verbrechens** oder möglichen gewerbs- oder gewohnheitsmäßigen **Vergehens**, Daten über die hieran möglicherweise beteiligten Personen eigens zu erheben. Nach dem Landesverwaltungsgesetz (§ 179 Abs. 2) müssen in jedem Einzelfall **Tatsachen** vorliegen. Allgemeine Erfahrungssätze ohne Bezug zum jeweiligen Geschehen sind nicht ausreichend.

Im Wortlaut: § 179 Abs. 2 LVwG
(2) Wenn Tatsachen dafür sprechen, daß ein
1. Verbrechen,
2. Vergehen gewerbsmäßig oder gewohnheitsmäßig begangen werden soll, können personenbezogene Daten erhoben werden über
a) Personen, bei denen Tatsachen dafür sprechen, daß sie solche Straftaten begehen oder sich hieran beteiligen werden,
b) Personen, bei denen Tatsachen dafür sprechen, daß sie Opfer solcher Straftaten werden, oder
c) Zeuginnen oder Zeugen, Hinweisgeber oder sonstige Auskunftspersonen, die dazu beitragen können, den Sachverhalt solcher Straftaten aufzuklären.

Die **Speicherpraxis** des Staatsschutzdezernates ging bislang in vielen Fällen an den präzisen Kriterien dieser Vorschrift vorbei. Sie wurde vielmehr als „Auffangnorm" benutzt, wenn sonstige Rechtsgrundlagen für Speicherungen nicht vorlagen. Insbesondere traf dies bei Daten über die Mitgliedschaft und die Aktivitäten von Personen in politischen bzw. extremistischen Vereinigungen und Bestrebungen zu. Da es sich hierbei um eine dem Verfassungsschutz zugewiesene **Vorfeldarbeit** handelte, die der Gesetzgeber der Polizei gerade nicht eröffnen wollte, war diese Datenverarbeitungspraxis zu beanstanden.

Beispiele:

- Zwölf Personen waren als „Mitglied einer als gewaltorientiert eingeschätzten ausländischen Organisation" gespeichert. Dem dazugehörigen Vorgang des Bundeskriminalamtes war hingegen zu entnehmen, daß „Hintergründe dieser Verbindungen bisher nicht konkretisiert werden konnten und nicht zur Einleitung eines Ermittlungsverfahrens führten".

- Im Zusammenhang mit Ermittlungen zu einem Brandanschlag wurde vom Verfassungsschutz eine Liste von Anhängern bzw. Sympathisanten von Ausländerorganisationen übermittelt. Obwohl nach den ausdrücklichen Feststellungen der Verfassungsschutzbehörde zu den in der Liste genannten Personen keine Hinweise auf ihre mögliche Tatbeteiligung vorlagen und auch die Ermittlungen keine Anhaltspunkte für ein polizeilich relevantes Verhalten ergaben, wurde zu jeder Person eine Personenakte angelegt.

• Unzulässige Vorratsdatenhaltung

In erheblichem Umfang wurden auch Daten über die **persönlichen Lebensumstände** über die Teilnahme an nicht verbotenen Versammlungen, Veranstaltungen, Aufrufen, Telefonaktionen der Medien sowie über die bei bestimmten Ereignissen festgestellten Kraftfahrzeuge in Personenakten gespeichert.

Beispiele:

- In einer Personenakte befand sich die Kopie des Personalausweises einer dritten Person. Sie hatte ihn vermutlich bei einer Gerichtsverhandlung gegen die Person, über die die Personenakte geführt wurde, verloren. Diese Registrierung der Teilnahme an der Gerichtsverhandlung verstieß nicht nur gegen die Persönlichkeitsrechte der Besucher, sondern auch gegen den Grundsatz der Öffentlichkeit des Strafverfahrens.

- In Form von Vermerken wurde zu einer Person, die in der Bundesrepublik bislang nicht durch strafrechtlich relevantes Verhalten aufgefallen war, gespeichert, daß sie mit einer minderjährigen Tochter in eine schleswig-holsteinische Stadt verzogen war. Es folgten Details über die Einschulung der Tochter, Vermerke über den Beginn einer Berufsausbildung und die Ausbildungsstätte der gespeicherten Person. Gespeichert war sogar, daß sie auf einem Weihnachtsmarkt an einem Stand Porzellanfiguren verkaufte und daß sie ein zweites Kind geboren hatte. Die Personalien ihres ständigen Lebensgefährten waren ebenfalls erfaßt.

- Zu einer Person fand sich ein Vermerk, in dem die Vermutung geäußert wurde, sie und eine Begleitperson seien lesbisch. Darüber hinaus waren bei dem Arbeitgeber Daten über ihre Ausbildung und ihren Arbeitsplatz erhoben worden.

Das polizeiliche Datenverarbeitungsrecht sieht allerdings eine Schwelle für die Verarbeitung von Daten aus dem persönlichen Umfeld polizeibekannter Personen vor. Demnach kommt die Speicherung von **„ergänzenden Erkenntnissen"** nicht schon dann in Betracht, wenn solche Erkenntnisse einmal potentiell „nützlich" sein könnten, sondern nur, wenn sie selbst gefahren- oder verdachtsbegründend sind.

Im Wortlaut:
Ziff. 4.5 KpS-Richtlinien
Bereits gespeicherte personenbezogene Unterlagen dürfen um Erkenntnisse ergänzt werden, die für sich alleine die Voraussetzungen einer Speicherung nicht erfüllen, wenn dies zur Erreichung des Sammlungszwecks oder zur Stützung einer Prognose über die Notwendigkeit der weiteren Speicherung der Unterlagen erforderlich ist.

- **Daten über dritte Personen**

In den Personenakten fanden sich zudem eine Vielzahl von Daten über dritte Personen, die zu der in der Akte gespeicherten Person bzw. dem dort festgehaltenen Ereignis in Beziehung standen (z.B. als Familienangehörige, Halter der von den gespeicherten Personen mitgenutzten Kraftfahrzeuge, Vermieter, Begleitpersonen, Hinweisgeber, Mittäter, aber auch als Personen, die sich zufällig im Umfeld der gespeicherten Person aufgehalten haben).

Dies kann sachlich nur gerechtfertigt sein, wenn es für die **Bewertung** der gespeicherten **„Hauptperson"** und des Sachverhaltes **unerläßlich** ist. In vielen Fällen wurden diese Grundsätze nicht beachtet.

Beispiele:

- In einer Personenakte wurden alle Eigentümer des von der gespeicherten Person gepachteten Restaurants namentlich, teilweise mit ihren Beschäftigungsstellen, genannt.

- Zu einer Person wurden Fernschreiben abgeheftet, aus denen sich Daten von möglichen Begleitpersonen, Kfz-Haltern, Vorbesitzern von genutzten Kfz, eines Wohnungsvoreigentümers, des Rechtsanwaltes eines anderen Häftlings sowie Angehöriger anderer Mitgefangener ergaben.

- **Prüffristen**

  Die gesetzlich angeordneten Prüffristen für Personenakten wurden vielfach nicht korrekt festgesetzt:

  - Sie wurden gar nicht oder falsch vergeben.

  - Es war nicht sichergestellt, daß die gesetzlichen Höchstgrenzen für Datenspeicherungen auch tatsächlich beachtet wurden.

  - Gründe, die die Festlegung einer neuen Prüffrist zur Folge hatten, waren nicht in der Personenakte notiert.

- **Speicherungen in der „Arbeitsdatei PIOS - Innere Sicherheit" (APIS)**

  In der Datei APIS werden „klassische" Staatsschutzdelikte, wie Hochverrat, verbotene Parteibetätigung, Sabotage, aber auch andere Delikte wie Sachbeschädigungen, Körperverletzungen oder Beleidigungen bundesweit erfaßt, wenn beim Täter eine extremistische Motivation erkennbar wird.

  In Schleswig-Holstein sieht die Errichtungsanordnung des Innenministers vor, daß stets zu prüfen ist, ob eine Speicherung in dieser bundesweiten Datei verhältnismäßig ist. Bei der Erfassung „**anderer Straftaten**" mit politischer Motivation ist stets die Schwere und die überörtliche Bedeutung der Tat ausschlaggebend.

  Eine stichprobenhafte Überprüfung der Speicherungspraxis zeigte einen weitgehend korrekten Umgang mit diesen personenbezogenen Daten. Auf unsere Anregung werden künftig alle in APIS eingestellten Vorgänge auch in der jeweiligen Personenakte dokumentiert.

- **Lichtbildkartei**

  Im Zeitpunkt der Prüfung umfaßte die Lichtbildkartei Fotos von insgesamt 320 Personen. Das Material datierte zu einem großen Teil bis in die 70er bzw. 80er Jahre zurück. In den betreffenden Personenakten war das Vorhandensein von Lichtbildern nicht vermerkt, so daß bei ihrer Vernichtung die Lichtbilder unzulässigerweise gespeichert bleiben.

  Ein weiterer häufig anzutreffender **Dokumentationsmangel** dieser Lichtbildkartei war, daß eine hinreichende Beschriftung der einzelnen Lichtbilder und Negative selbst nicht existierte. So enthielt ein Lichtbildumschlag 51 Reproduktionen eines Lichtbildes, die gänzlich unbeschriftet waren. Gefunden wurden auch Lichtbilder, obwohl in der

Personenakte ausdrücklich vermerkt war: „Fotos zur Person nicht vorhanden."

Bei einer derartigen Dokumentation war es dann keine besondere Überraschung, als wir zu einer Person Lichtbilder aus einer erkennungsdienstlichen Behandlung vorfanden, obwohl das Landeskriminalamt im Rahmen einer Eingabe dieser Person zuvor schriftlich bestätigt hatte, es liege kein erkennungsdienstliches Material mehr in Schleswig-Holstein vor.

- **Datenspeicherungen über gefährdete Personen**

  Daten über gefährdete Personen, aber auch über Personen, von denen Gefährdungen ausgehen können (Gefährder), werden in Gefährdeten- und Gefährderakten sowie einer speziellen Datei vorgehalten.

  Auffällig war, daß zwischen dieser Datei und der Aktensammlung keine Kongruenz bestand, so daß keine Datensammlung für sich vollständige Auskunft über den jeweiligen Datenbestand dieser Personengruppen geben konnte. Darüber hinaus war der Aktenbestand stark veraltet, weil wegen **mangelnder Prüffristenüberwachung** bislang keine Aktualisierung erfolgte.

  Die Speicherung von Daten in einer Gefährdetenakte ist zudem nur nach vorheriger Aufklärung des Betroffenen und mit seiner schriftlichen Einwilligung zulässig, sofern nicht eine unmittelbare, konkrete Gefahr vorliegt. Bei einer Vielzahl der Gefährdetenakten fehlte diese schriftliche Einwilligungserklärung.

  Außerdem befanden sich in den Akten in beträchtlichem Umfang Daten über dritte Personen, die bei der Überprüfung möglicherweise gefährdungsrelevanter Sachverhalte einmal festgestellt worden waren. Offensichtlich wurde für diesen Personenkreis **keine ordentliche Datenpflege** mit regelmäßigen Prüfungen hinsichtlich der Erforderlichkeit ihrer Weiterspeicherungen durchgeführt.

  Beispiele:

  - Die Personalien und Kraftfahrzeugdaten eines Schornsteinfegers wurden gespeichert, weil dieser bei Messungen sein Auto regelmäßig entlang der Anfahrtsroute einer gefährdeten Person geparkt hatte.

  - In einer anderen Gefährdetenakte waren Mitmieter dieser gefährdeten Person ebenso gespeichert wie Halter von Kraftfahrzeugen, die in der Nähe des Betriebes der gefährdeten Person parkten. Erfaßt waren auch ein Landwirt, der an einer Treibjagd teilgenom-

men hatte, ein Betriebsangehöriger, der auf dem Betriebsgelände fotografiert hatte, aber auch Lieferanten des Gefährdeten.

- **Häftlingsüberwachung**

Nach geltender Rechtslage besitzt nur der **Leiter der Justizvollzugsanstalt** (bei Untersuchungshaft nur ein Haftrichter) die Kompetenz, eine Überwachung der Besuche und des Schriftwechsels mit Gefangenen anzuordnen. Er kann sich bei der Überwachung der Amtshilfe durch die Polizei bedienen.

Stichwort: Häftlingsüberwachung
Aus Gründen der Behandlung oder der Sicherheit und Ordnung der Haftanstalt, dürfen nach den Bestimmungen des Strafvollzugsgesetzes Besuche und Schriftverkehr von Strafgefangenen überwacht werden. Eine entsprechende Überwachung von Untersuchungshäftlingen ist auf der Grundlage der Strafprozeßordnung möglich.

Die Prüfung zeigte, daß die Praxis der Polizei dem allerdings nicht entsprach. Die **Besuchsüberwachung** wurde nämlich **eigenständig** von der **Polizei** durchgeführt, ohne daß weitere Entscheidungen durch den Anstaltsleiter der Justizvollzugsanstalt (JVA) getroffen wurden. Das vom anwesenden Polizeibeamten aufgrund seiner Notizen gefertigte Besuchsprotokoll verblieb beim Landeskriminalamt und wurde zeitgleich an die JVA und an andere polizeiliche Dienststellen gesandt. Eine vorherige Sichtung und Relevanzprüfung im Hinblick auf den eigentlichen Überwachungszweck durch den Leiter der JVA fand offensichtlich nicht statt.

Die **Besuchsprotokolle** enthielten in vielen Fällen Informationen, deren Erforderlichkeit im Hinblick auf den Zweck der Datenerhebung nicht nachvollziehbar war.

Entgegen der anläßlich einer früheren Prüfung (vgl. 16. TB, Tz. 4.3.3) gegebenen Zusicherung des Justizministeriums, wonach „die Weitergabe von Kopien von Briefen an das Kriminalpolizeiamt gemäß ausdrücklicher Weisung seit vielen Jahren, insbesondere seit Inkrafttreten datenschutzrechtlicher Bestimmungen in Schleswig-Holstein, nicht mehr praktiziert“ werde, fanden sich in den polizeilichen Unterlagen zur Häftlingsüberwachung mehrere **Kopien von Briefen** an Häftlinge, die von der JVA an das Landeskriminalamt weitergegeben worden sind, das wiederum Kopien an das Bundeskriminalamt und den Polizeipräsidenten eines anderen Bundeslandes übermittelte.

Unter anderem fanden wir Briefe, in denen höchstpersönliche Angaben enthalten waren, beispielsweise einen 19seitigen Brief, der einen Abriß über die Kindheit des Absenders, seinen politischen Werdegang, aber auch seine sexuelle Orientierung wiedergab. Wir haben ihre

Vernichtung verlangt. Da diesen Briefen Anhaltspunkte für Straftaten nicht zu entnehmen waren, stellte ihre Weitergabe und Speicherung in den polizeilichen Unterlagen nämlich einen unzulässigen, tiefen Eingriff in das Persönlichkeitsrecht des Absenders dar.

Die Reaktion des Innenministers

Der Innenminister hat auf den Prüfbericht schnell und in der Sache angemessen reagiert. Inzwischen sind 169 von insgesamt 206 beanstandeten Einzelfällen bereinigt. Der Datenbestand zu den verbliebenen 37 Einzelbeispielen war zunächst vorsorglich gesperrt worden, da hierzu noch Erörterungsbedarf mit uns gesehen wurde.

Auch hinsichtlich der rechtlichen Bewertung dieser Fälle ist zwischenzeitlich weitgehender Konsens erzielt worden, so daß nunmehr eine Bereinigung des gesperrten Datenbestandes zu erwarten ist. Ein weiteres Ergebnis der Besprechung ist, daß die Speicherung künftig nach klareren Kriterien erfolgen soll, die nachvollziehbar dokumentiert werden. Lediglich einige Detailfragen zu Datenerhebungen und -speicherungen bedürfen nun noch der Klärung. Die Häftlingsüberwachung wird in Abstimmung mit dem Justizministerium neu geregelt.

Auch außerhalb des geprüften Bereiches ist inzwischen mit umfangreichen Bereinigungsarbeiten begonnen worden.

4.2.2 Prüfung einer Polizeiinspektion

Bei der Prüfung einer Polizeidienststelle erwies sich einmal mehr die Art und Weise der Führung der Kriminalakten als wesentlicher Kritikpunkt.

Bei einer datenschutzrechtlichen Querschnittsprüfung in einer Polizeiinspektion konnten wir Qualitätsunterschiede bei der Erhebung und Verarbeitung personenbezogener Daten in den einzelnen Organisationseinheiten feststellen:

- **Einsatzleitstelle**

  Alle bei der Einsatzleitstelle unter den Notrufnummern 110 und 112 eingehenden Telefonanrufe **wurden automatisch** aufgezeichnet und die Tonbänder circa zwei Monate aufbewahrt. Anrufer, die zum Ausdruck brachten, daß sie eine Telefonaufzeichnung nicht wünschten, wurden auf die Möglichkeit hingewiesen, sich unter einer anderen Telefonnummer bei der Polizeidienststelle zu melden. Dieses Verfahren war nicht zu beanstanden.

Die den Funkstreifen bekanntgewordenen oder mitgeteilten Sachverhalte wurden in **Einsatzberichten** formularmäßig festgehalten. Darin wurden neben einer umfassenden und einheitlichen Einsatzdokumentation auch etwaige Anfragen in Zentral- und Fremdverfahren (u.a. PED, ZEVIS, EIS) registriert. Wir mußten aber bemängeln, daß die Dokumentation des Abfragegrundes und/oder eine Sachverhaltsdarstellung nicht immer hinreichend erfolgt ist, so daß eine Kontrolle der Rechtmäßigkeit der Datenabrufe kaum möglich war. Erfreulich war aber der geringe Umfang personenbezogener Daten in den Einsatzberichten.

Stichwort:
Polizeiliche Erkenntnisdatei (PED)
Die PED ist das wichtigste automatisierte Informationssystem der Landespolizei. In ihr sind Personen gespeichert, über die eine Kriminalakte angelegt ist oder die zur Fahndung ausgeschrieben sind.

Einwohnerinformationssystem (EIS)
Nach den Vorschriften des Melderechts sind die Kommunen und Kreise verpflichtet, einen bestimmten Teil der Meldedaten der Polizei zur Verfügung zu stellen. Mit Hilfe des zentralen EDV-Verfahrens EIS kommen viele Gemeinden und Kreise dieser Verpflichtung nach. Die Polizei kann über EIS rund um die Uhr on line auf die Daten zugreifen.

Zentrales Verkehrsinformationssystem (ZEVIS)
Zentrales Verkehrsinformationssystem. ZEVIS ist ein automatisiertes Auskunftssystem, mit dem bestimmte Behörden beim Kraftfahrt-Bundesamt in Flensburg auf Daten von ca. 40 Millionen Kraftfahrzeughaltern zugreifen können. Die Anfrage kann u.a. mit dem Kennzeichen, Kennzeichenfragmenten oder mit dem Namen erfolgen..

- **Polizeistation**

  Bei der stichprobenweisen Überprüfung von **Vorgangsdurchschriften** der Polizeistation war folgendes zu bemängeln:

  - Die polizeiliche Erkenntnisdatei (PED) war zu einem Zeugen abgefragt worden, obwohl es ohne besondere Begründung nicht zulässig ist, die Daten von Zeugen mit polizeilichen Dateien abzugleichen.

  - Dem Verfassungsschutz wurde im Rahmen einer Sicherheitsüberprüfung ein Vorfall der Nötigung und Straßenverkehrsgefährdung mitgeteilt, bei dem der Betroffene jedoch Geschädigter war. Dies begründete keinesfalls einen sicherheitsrelevanten Umstand. Die Übermittlung war mithin unzulässig.

- **Kriminalpolizeistelle**

  Die Kontrolle von **Kriminalakten** gab zu erheblichen datenschutzrechtlichen Beanstandungen Anlaß. Kriminalakten dürfen nach der Gesetzeslage (siehe Wortlaut v. § 189 LVwG auf S. 25) nur angelegt

werden, wenn eine Wiederholungsgefahr besteht und eine Prognose im Hinblick auf die Täterpersönlichkeit vorliegt. Keinesfalls ist es zulässig, pauschal alle im Verlauf von Ermittlungsverfahren anfallenden Daten zu speichern. Vielmehr bedarf es eines besonderen Auswertungsschrittes durch den zuständigen Sachbearbeiter, der zur Erstellung eines entsprechenden Merkblattes führt, das die auf die präventiven Zwecke abgestimmte Sachverhaltsschilderung enthält.

Folgende Unterlagen gehören nach der KA-Regelung nicht in eine Kriminalakte:

- Ausschreibungs- und Fahndungsunterlagen
- Schlußberichte der Staatsanwaltschaft
- Durchschriften von Strafanzeigen
- Vernehmungsniederschriften
- Haftbefehle
- Auszüge aus EIS und ZEVIS
- PED-Ausdrucke
- Bundeszentralregisterauszüge, es sei denn, hierdurch wird eine den derzeitigen Überprüfungsfristen zugrundeliegende Prognoseentscheidung belegt (Ziff. 5.1 KA-Regelung)

Bei der Speicherung von **Daten über dritte Personen** (z.B. Zeugen, Geschädigte, Anzeigenerstatter) muß ein besonders restriktiver Maßstab angelegt werden. Solche Daten dürfen nur dann enthalten sein, wenn dies unerläßlich ist. Dies gilt z.B. für Mittäter; keinesfalls jedoch für Rechtsanwälte oder Wohnungsvermieter der Verdächtigen.

Der Ausgang des Ermittlungsverfahrens bzw. das **Ergebnis der Gerichtsverhandlung** ist zeitnah zu erfassen, um festzustellen, ob weiterhin von einem verbliebenen Tatverdacht und einer Wiederholungsgefahr ausgegangen werden kann. Nur dann ist eine weitere Datenspeicherung rechtlich zulässig.

Werden Personen **erkennungsdienstlich behandelt**, ist die Begründung hierfür unter Angabe der Rechtsgrundlage in der Kriminalakte zu dokumentieren. Aber auch die Anzahl der in diesem Zusammenhang gefertigten Lichtbilder, die sich in der Kriminalakte selbst oder in anderen Sammlungen befinden, muß dokumentiert werden. Die Lichtbilder sind mit den Personalien des Betreffenden zu kennzeichnen, um ihre Vernichtung zum gegebenen Zeitpunkt zu gewährleisten. Auch dies wurde in einer Reihe von Fällen nicht beachtet.

Darüber hinaus mußte die **Datensicherheit** bemängelt werden. So fanden sich im Zeitpunkt unserer Prüfung in unabgeschlossenen Schränken auf dem Flur Asservate, die mit Namen von Tatverdächtigen beschriftet waren. In Räumen, in denen auch Vernehmungen durchgeführt werden, standen nicht abgeschlossene Schränke und

Regale mit Aktenordnern, die Namen von Beschuldigten und Opfern aufwiesen.

Die Reaktion des Innenministers

Der Innenminister hat mitgeteilt, daß unseren Forderungen und Anregungen weitgehend gefolgt wird. Die geprüften Kriminalakten sind bereits entsprechend bereinigt worden. Bei der Kriminalpolizeistelle sind organisatorische Maßnahmen durchgeführt worden, die die Datensicherheit nunmehr gewährleisten sollen.

4.2.3 INPOL-Neu: mit dem Rasenmäher durch die Landespolizeigesetze?

Der Bund will das polizeiliche Informationssystem INPOL neu gestalten. Die bisher vorliegende Konzeption und der Entwurf des BKA-Gesetzes führen zu einer verfassungsrechtlich bedenklichen Verschiebung von Zuständigkeiten weg von den Ländern hin zum Bund.

Das Bundesministerium des Innern plant, das wichtigste System der polizeilichen Informationsverarbeitung, **INPOL**, mit dem Bund und Länder gemeinsam arbeiten, neu zu gestalten. Neben einer technischen Neukonzeption sind vor allem umfangreiche Ausweitungen der Speicherbefugnisse vorgesehen. Diese sollen rechtlich durch eine Neufassung des Bundeskriminalamtgesetzes abgesichert werden. Die dort vorgesehenen Regelungen zur Behandlung der Daten, die von den Polizeien der Länder angeliefert werden, und die weiteren Vorstellungen im Rahmen von INPOL-Neu sind unserer Ansicht nach nicht mit dem Grundgesetz vereinbar. Nach der verfassungsmäßigen Kompetenzverteilung liegt die Gesetzgebungsbefugnis zur Gefahrenabwehr grundsätzlich bei den Ländern. Die Gesetzgebung des Bundes darf lediglich den Bereich der Zusammenarbeit des Bundes und der Länder in Angelegenheiten der Kriminalpolizei regeln.

> ***Stichwort: INPOL***
> *INPOL ist das gemeinsame Informationssystem des Bundes und der Länder. Hierzu gehören beispielsweise folgende Anwendungen:*
> - *Personenfahndung*
> - *Sachfahndung*
> - *Haftdatei*
> - *Erkennungsdienst*
> - *Arbeitsdateien für besondere Kriminalitätsbereiche (PIOS)*

Die im **BKA-Gesetzentwurf** vorgesehenen Regelungen gehen jedoch weit darüber hinaus. Sie legen fest, welche Daten die Länder in das INPOL-System einstellen müssen. Dies wären wesentlich mehr als derzeit nach dem schleswig-holsteinischen Polizeigesetz zulässig. So ist z.B. vorgesehen, die Daten Dritter zu speichern, die Personen, die einer Straftat verdächtig sind, lediglich begleitet haben oder mit diesen zufällig in

Kontakt standen. Davon wäre eine große Anzahl Unverdächtiger betroffen.

Problematisch ist außerdem die Frage, wann die gespeicherten Daten gelöscht werden müssen. Es ist vorgesehen, daß im Regelfall nach zehn Jahren geprüft wird, ob eine Speicherung noch aufrechterhalten werden muß. Das schleswig-holsteinische Landesrecht sieht hier eine deutlich kürzere Prüffrist von fünf Jahren vor. Nach unserer Auffassung kann die Zehnjahresfrist nur als Höchstgrenze gelten, d.h., eine kürzere Prüffrist und die darauf folgende Löschung nach Landesrecht muß den am INPOL-Verbund angeschlossenen Polizeibehörden unbenommen bleiben, weil die Stelle für die eingespeicherten Daten verantwortlich ist, von der die Daten ursprünglich stammen.

Das Innenministerium des Landes Schleswig-Holstein hat sich allerdings bislang auf den Standpunkt gestellt, die Zulässigkeit der Speicherung von Daten im INPOL-Verbundsystem werde sich allein nach den Vorgaben des künftigen BKA-Gesetzes richten. Auch die Prüf- und Löschungsfristen müßten allein den Regelungen des Bundesgesetzes entnommen werden. Diese Auffassung würde nach unserer Ansicht zu Speicherungen führen, die nach dem Polizeirecht des Landes Schleswig-Holstein nicht zulässig sind.

Was ist zu tun?
Das Innenministerium des Landes Schleswig-Holstein sollte seine Auffassung überdenken und auf eine der grundgesetzlichen Zuständigkeitsverteilung entsprechende Aufgabenbeschreibung im BKA-Gesetzentwurf hinwirken.

4.2.4 COMPAS

Eingehende Beratungen haben zu weiteren wesentlichen datenschutzrechtlichen und technischen Verbesserungen beim Projekt COMPAS geführt.

Waren in der Konzeption des „computergestützten polizeilichen Arbeitsplatzsystems“ COMPAS zunächst eine Reihe von datenschutzrechtlichen Schwachpunkten erkennbar, so ist der Innenminister unseren Änderungs- oder Klarstellungsvorschlägen (vgl. 18. TB, Tz. 4.2.8) zwischenzeitlich weitgehend gefolgt.

Beispiele:

- Durch Dienstanweisung wird geregelt, daß in COMPAS nur Daten erfaßt werden dürfen, die für die Bearbeitung des Einzelfalles tatsächlich benötigt werden. Die Speicherung von Personenbeschreibungen

muß z.B. besonders begründet werden, wenn sich die Erforderlichkeit nicht bereits aus dem zugrundeliegenden Sachverhalt ergibt.

- Um bei COMPAS eine Synchronisation mit dem papierenen Datenbestand zu gewährleisten, ist verfahrenstechnisch sichergestellt worden, daß Änderungen im Datenbestand erst vollzogen werden, wenn zuvor ein papierener Ausdruck erfolgt ist. Darüber hinaus ist in die Fußzeile aller Vordrucke ein Druckdatum eingefügt, so daß eine zusätzliche Kontrollmöglichkeit vorhanden ist. In einer Dienstanweisung wird ausdrücklich darauf hingewiesen, daß bei Abweichungen die auf dem Papier vorhandenen Daten als authentisch anzusehen sind.

Was ist zu tun?
Der Innenminister muß dafür Sorge tragen, daß die Vorschriften zu COMPAS auch in der Praxis zum Tragen kommen.

4.2.5 POLDOK

Der Innenminister hat den Erlaß zum POLDOK-Meldedienst trotz unserer datenschutzrechtlichen Kritik in Kraft gesetzt. Er trägt weder datenschutzrechtlichen Belangen Rechnung, noch genügt er offenbar den Anforderungen der polizeilichen Praxis.

Zum neuen POLDOK-Meldedienst erreichten uns Anfragen von irritierten Polizeibeamten. Sie konnten nicht verstehen, aus welchem Grunde die Personendaten der Beschuldigten dort durch ein Aktenzeichen ersetzt werden, während gleichzeitig die Opferdaten gespeichert bleiben sollen. Die Recherche nach Opfern und Geschädigten komme extrem selten vor. Allerdings erschwere es die alltägliche Arbeit erheblich, daß jetzt nicht mehr nach den Beschuldigten mit Namen, sondern umständlich über das Aktenzeichen und dann mit diesem in POLDOK der dazugehörige Datensatz gesucht werden müsse.

Der Erlaß ist auch aus datenschutzrechtlichen Gründen zu kritisieren:

- Eine Speicherung personenbezogener Daten von **Tätern** oder **Tatverdächtigen** nach Abschluß eines Ermittlungsverfahrens kann nur nach den Regelungen des Landesverwaltungsgesetzes erfolgen. Dies wird jedoch nicht dadurch erreicht, daß der Name des Verdächtigen durch das Aktenzeichen der Staatsanwaltschaft - wie im Erlaß vorgesehen - ersetzt wird. Denn auch hierdurch bleibt die betreffende Person eindeutig, wenn auch etwas umständlich, bestimmbar. Ein solcher Datensatz enthält also auch weiterhin personenbezogene Daten. Unabdingbar ist es vielmehr, daß die Prüffristen des LVwG eingehalten werden. Der Verfahrensausgang ist außerdem spätestens zwei Jahre nach Abgabe an die Staatsanwaltschaft zu ermitteln.

- Bei Daten von **Opfern und Geschädigten** muß eine weitergehende Einschränkung der Speicherungsdauer erfolgen. Opferdaten können allenfalls bis zum Abschluß eines Strafverfahrens gespeichert bleiben. Spätestens mit der Verurteilung eines Täters ist die Weiterspeicherung für Ermittlungszwecke nicht mehr erforderlich.

- Der **Katalog der meldepflichtigen Straftaten** ist erheblich zu weit gefaßt und schließt auch typische Massendelikte, wie z.B. Trickdiebstahl, Diebstähle in und aus öffentlichen Verkehrsmitteln, Werbe- und Verkaufsbetrug, betrügerische Vermittlung von Aufträgen und Lieferungen, mit ein, für die die Erforderlichkeit einer landesweiten Datenspeicherung keinesfalls gesehen wird.

Wir haben die Polizeibeamten darauf hingewiesen, daß die im Erlaß festgeschriebene Verfahrensweise nicht auf unsere Einflußnahme zurückgeht. Unserer Auffassung nach wäre es vielmehr datenschutzrechtlich nicht zu beanstanden, wenn die Personendaten von Beschuldigten für den rechtlich zulässigen Zeitraum speichert blieben. Die dauerhafte Speicherung der Opferdaten ist für uns ebenso unakzeptabel wie offenbar für einige Polizeipraktiker unverständlich.

Was ist zu tun?

Der Innenminister sollte den POLDOK-Erlaß noch einmal überprüfen und die genannten Schwächen beseitigen.

4.3 Verfassungsschutz - NADIS-Datensatz

Die Personenzentraldatei im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden (NADIS) wird entgegen den Bestimmungen im Bundesverfassungsschutzgesetz nicht nur als System zum Wiederauffinden von Akten, sondern auch als eine Recherchedatei für operative Zwecke des Geheimdienstes genutzt.

Im 16. Tätigkeitsbericht (vgl. Tz. 4.1.2.2) hatten wir kritisiert, daß durch die neuen Richtlinien zu NADIS die Vorgaben des Bundesverfassungsschutzgesetzes (BVerfSchG) überschritten werden. Trotz unserer Kritik sind die Richtlinien inzwischen in Kraft getreten.

Dies hat zur Folge, daß in der Personenzentraldatei (PZD) beim Bundesamt für Verfassungsschutz neben den eigentlichen Personalien unter anderem auch Angaben zu **Kraftfahrzeugen**, **Schließfach-**, **Konto-** und **Telefonnummern** gespeichert werden. Eine so weitgehende Speicherung

steht mit den Vorschriften des BVerfSchG nicht in Einklang. Danach dürfen derartige Dateien nur Daten enthalten, „die zum Auffinden von Akten und der dazu notwendigen **Identifizierung von Personen** erforderlich sind". Hierzu sind nach unserer Auffassung die „klassischen" Personenangaben ausreichend. Dies sind Vor- und Zuname, Geburtsname, Tag und Ort der Geburt, Familienstand, Beruf, Wohnort und Staatsangehörigkeit.

Im Wortlaut:
§ 6 Satz 1 u. 2 BVerfSchG
Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für den Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach § 5 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind.

Das Bundesamt für den Verfassungsschutz argumentiert, manchmal sei eben der Name nicht bekannt. In solchen Fällen könne man Personen auch mit Hilfe von Kfz-, Konto- oder Schließfachnummern identifzieren. Würde man diese Begründung akzeptieren, so wäre der Speicherung weiterer unterschiedlichster **Personenmerkmale** Tür und Tor geöffnet. Am Ende könnte die Suchmöglichkeit z.B. nach allen Personen mit roten Haaren, Brille, bestimmten Eigenschaften, Neigungen stehen. Für Recherchen dieser Art steht den Verfassungsschutzbehörden ein eigenes Verfahren zur Verfügung, das allerdings an engere gesetzliche Voraussetzungen gebunden ist.

Was ist zu tun?
Die schleswig-holsteinische Verfassungsschutzbehörde sollte die Eingaben in die PZD auf das gesetzlich zulässige Maß beschränken. An die zu weiten Richtlinien des Bundesamtes ist sie nicht gebunden.

4.4 Justizverwaltung

4.4.1 MEGA

Der Justizminister ist dabei, die Gerichte in großem Umfang mit Computern auszustatten. Mängel in der Konzeption und vor allem das Fehlen einer ausführlichen Dokumentation des Verfahrens erschweren die datenschutzrechtliche Bewertung. In einzelnen Teilen sind Nachbesserungen erforderlich, grundsätzliche Bedenken gegen MEGA bestehen jedoch nicht.

Im 18. Tätigkeitsbericht (vgl. Tz. 5.1) wurde über die Einführung des Systems MEGA als Pilotprojekt und die dabei aus unserer Sicht zu beachtenden Maßgaben berichtet. Das Projekt hat mittlerweile die Pilotphase verlassen und läuft bereits bei acht Amtsgerichten im **„Echtbetrieb"**.

Ein Besuch bei einem dieser Gerichte erbrachte, daß den datenschutzrechtlichen Belangen im wesentlichen genügt wird. Allerdings ergaben sich neue Fragestellungen, die noch nicht abschließend geklärt werden konnten.

In dem betreffenden Gericht sind 60 EDV-Arbeitsplätze installiert. Auf circa 40 Arbeitsplätzen läuft die Anwendung MEGA einschließlich eines Paketes mit Standardsoftware zur Textverarbeitung, zum Nachrichtenaustausch, zum Faxen vom PC und zur Tabellenkalkulation. Daneben werden spezielle Programme für besondere juristische Anwendungen vorgehalten. Auf 20 Arbeitsplätzen wird nur Standardsoftware eingesetzt. Der Betrieb so vieler Verfahren bringt es mit sich, daß an unterschiedlichen Stellen im System personenbezogene Daten gespeichert werden. Zwar sind im Rahmen von MEGA Vorkehrungen getroffen, um eine fristgemäße Löschung von Daten zu gewährleisten. Diese laufen jedoch leer, wenn Datensätze auch unter anderen Programmen angelegt werden. Bisher fehlt es an einem schlüssigen Konzept, wie **unkontrollierte Mehrfachspeicherungen** verhindert werden könnten.

Stichwort: MEGA
*MEGA ist die Abkürzung für **M**ehr**l**änder-**G**erichts-**A**utomation. So nennen die Bundesländer Brandenburg, Schleswig-Holstein und Thüringen ihr gemeinsam neu entwickeltes EDV-Verfahren für die Gerichte. Es soll erstmalig in der deutschen Justiz die vollständige Einbindung der Arbeitsplätze von Richtern und Rechtspflegern, Aktenverwaltung und Schreibdienst verwirklichen. Vor allem für die vielen kleinen Gerichte erhofft man sich damit eine deutliche Verbesserung der Arbeitsbedingungen u.a. durch den Wegfall von Transportwegen, weniger Zeitaufwand für Absprachen und schnellere Erledigung von Schreibarbeiten. Den Richtern sollen bessere Informationsmöglichkeiten (z.B. durch die Abfrage von juristischen Datenbanken) die Entscheidungsfindung erleichtern.*

Zum Verfahren MEGA selbst ist positiv hervorzuheben, daß der **Zugriff** auf Daten zu Personen deutlich **beschränkt** ist. Jeder Anwender kann nur die Funktionen nutzen, mit denen er dienstlich befaßt ist. Der Richter oder die zu seiner Serviceeinheit gehörenden Mitarbeiter können nur Verfahren des Verfahrenszweigs aufrufen, der ihnen laut Geschäftsverteilungsplan zugeordnet ist, z.B. nur Verfahren des Familienrechts. Zugriff auf Datenspeicherungen in sonstigen, z.B. strafrechtlichen Verfahren haben sie nicht. Innerhalb dieser Begrenzung ist es möglich, nach Verfahren zu suchen, indem entweder ein Aktenzeichen oder die Personendaten eines unmittelbar am Verfahren Beteiligten (also im Zivilverfahren einer Partei bzw. im Strafverfahren des Angeklagten) eingegeben werden. Erst wenn ein konkretes Verfahren aufgerufen ist, lassen sich weitere am Verfahren teilnehmende Personen, wie z.B. Zeugen, anzeigen. Ein Zugriff auf die in einer Datenbank gespeicherten gesamten Datenbestände in Tabellenform ist den Anwendern von MEGA nicht möglich.

Vorgesehen ist auch, daß der größte Teil der Daten gelöscht wird, wenn ein Verfahren abgeschlossen ist oder nicht weiter betrieben wird. In den papierenen Akten wird dieser Zustand dokumentiert, indem die Akte „**weggelegt**" wird. In MEGA soll der Großteil der Daten im Januar des übernächsten Jahres nach dem Eintragen der Weglege-Verfügung gelöscht werden. Übrig bleiben dann nur die Namen der unmittelbar Verfahrensbeteiligten sowie die Aktenzeichen. Diese Daten sollen dazu dienen, die weggelegte Akte im Register wiederzufinden. Sie werden gelöscht, wenn die Akte vernichtet wird. Wann dies der Fall ist, richtet sich zur Zeit noch nach den **Aufbewahrungsbestimmungen** für die Justiz. Da hierbei zum Teil sehr langfristige Speicherungen vorgesehen sind (zu den daraus resultierenden Problemen vgl. auch Tz. 5.2), wird von den Datenschutzbeauftragten schon seit längerem gefordert, daß diese überprüft und in Form eines Gesetzes getroffen werden müssen. Dabei sollten die zum Teil überlangen Aufbewahrungsfristen verkürzt werden. Ob die zunächst vorgesehene Reduzierung („Rumpfung") der Daten sowie die spätere vollständige Löschung funktioniert, konnte noch nicht geprüft werden, da das System MEGA sich an dem besuchten Gericht erst seit kurzem im Einsatz befand und die Löschungs- bzw. Rumpfungsfristen noch nicht erreicht waren.

Im 18. Tätigkeitsbericht (vgl. Tz. 5.1) hatten wir uns kritisch zu den sogenannten „**persönlichen Textfeldern**" geäußert. Es handelt sich dabei um Datenfelder, die jeweils mit einem Verfahrensdatensatz verbunden sind und die Eingabe eines beliebigen Textes ermöglichen. Das Justizministerium hat erklärt, diese Felder sollten dazu dienen, persönliche Notizen zu Zwischenergebnissen bei der Rechtsfindung der Richter und Rechtspfleger, die bisher in Papierform vorgenommen und traditionell in einer Tasche des Aktendeckels aufbewahrt wurden, auch im System MEGA zu ermöglichen. Positiv hervorzuheben ist, daß die Speicherungen in diesem Feld an die Speicherfristen der übrigen verfahrensbezogenen Daten geknüpft sind. Bei der automatischen Rumpfung der Daten werden auch die dort niedergelegten Informationen gelöscht. Damit ist diese Methode der Speicherung von Notizen zum Verfahren gegenüber einer unbegrenzten und kaum kontrollierbaren Speicherung von Notizen, die mit einer Standardtextverarbeitung erstellt und an anderer Stelle im System abgelegt werden, vorzuziehen.

Während sich im 18. Tätigkeitsbericht noch die Aussage findet, ein **landesweiter Zugriff** auf die Gerichtsdaten sei ausgeschlossen, belehrte uns der Besuch bei dem Amtsgericht eines anderen. Sämtliche Amtsgerichte werden nämlich mit dem Justizministerium in Kiel und auch untereinander über **Telekommunikationsverbindungen** kommunizieren können. Dabei sollen von Kiel aus neue Programmteile eingespielt und technische Unterstützung gegeben werden. Vom Justizministerium aus besteht auch Zugriff auf die Datenbanken, in denen die Daten der in MEGA erfaßten Verfahren gespeichert sind. Für äußerst problematisch

halten wir dabei, daß Zugriffe jedenfalls theoretisch auch vorgenommen werden können, ohne daß es am jeweiligen Amtsgericht bemerkt wird. Zwar versucht man im Justizministerium, u.a. durch Anwendung des Vier-Augen-Prinzips, Mißbräuche auszuschließen. Es ergibt sich jedoch eine nicht zu unterschätzende Gefährdung für die Integrität der Daten aus gerichtlichen Verfahren und für das informationelle Selbstbestimmungsrecht der an Gerichtsverfahren beteiligten Bürger. Auch Fragen der Unabhängigkeit der Gerichte sind berührt. Hier müssen noch weitergehende Erörterungen mit dem Justizminister stattfinden.

Bemerkenswert ist darüber hinaus, daß die IT-Kommission des Landes im Juli 1996 im Umlaufverfahren (d.h. ohne jede Erörterung) ihre Zustimmung dazu gab, daß das Verfahren von der **Pilotphase** an einem Amtsgericht in die **„flächendeckende" Einführungsphase** bei allen Gerichten überführt wurde. Wenn dem allgemeinen Einsatz eines automatisierten Verfahrens schon ein Pilotversuch vorangestellt wird, in dem de facto mit echten Daten getestet wird (vgl. die grundsätzliche Kritik im 18. TB, Tz. 6.3), so hätte man erwarten können, daß am Ende dieses Tests ein Erfahrungsbericht gestanden hätte, daß Schlußfolgerungen und evtl. Modifikationen dokumentiert worden wären und daß vor allen Dingen ein in sicherheitstechnischer und organisatorischer Hinsicht **abschließend definiertes** Verfahren zum Echteinsatz gelangt.

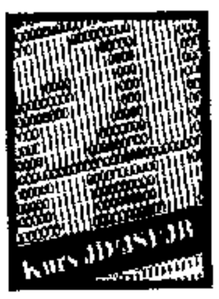
Da wir in der IT-Kommission nur mit beratender Stimme vertreten sind, konnten wir in dem o.a. Umlaufverfahren kein Votum abgeben. Wir haben dem Ministerium deshalb unsere **Vorbehalte** gegen das zu vage Sicherheitskonzept schriftlich dargelegt. Sie beziehen sich insbesondere darauf, daß nach den Planungen wesentliche Teile der **Programmentwicklung und Systembetreuung** bei den IT-Stellen vor Ort bzw. bei den Mittelinstanzen angesiedelt werden. Hierzu sollen u.a. folgende Teilfunktionen gehören:

- Entwicklung von Fachanwendungen auf örtlichen IT-Systemen nach Anforderungen der Benutzer
- Entwurf von Anwendungslösungen
- Programmtest
- Entwicklung von Anwendungen zur Büroautomation/-kommunikation auf örtlichen IT-Systemen unter Verwendung von Standardprogrammen zur individuellen Datenverarbeitung nach Anforderungen der Nutzer
- Übernahme der Anforderungen der Nutzer in Vorgaben- und Pflichtenheften
- Einrichtung der Software zur „Individuellen Datenverarbeitung" (IDV)
- Test von IDV-Lösungen
- Freigabe und Dokumentation von IDV-Lösungen
- Überwachung von Hardware-Systemen

- Systembetreuung Software
- Systembetreuung Netze
- Schaffung der Voraussetzungen für den Netzbetrieb
- Konzeption und Realisierung von Sicherheitsmaßnahmen
- Prüfung von Sicherheitsmaßnahmen
- Systemüberwachung
- Fehlerbehandlung
- Planung und Kontrolle des Produktionsablaufes und der Produktionsergebnisse
- Überwachung der Auftragsabwicklung
- Benutzerverwaltung

Ein solch breites Aufgabenspektrum dürfte in den Gerichten **erhebliche aufbau- und ablauforganisatorische Veränderungen** gegenüber der papierorientierten Verwaltung zur Folge haben.

Allerdings sind nach unserem Kenntnisstand auch in den Gerichten, die bereits mit den technischen Systemen unter „Echtbedingungen" arbeiten, intern weder die administrativen Zuständigkeiten festgelegt noch die allgemeinen und speziellen Dienstanweisungen für die Behördenleitung und die einzelnen Funktionsträger in Kraft gesetzt worden. Die Teilverfahren „Textbearbeitung", „Tabellenkalkulation", „E-Mail" und „Fax via PC" werden daher in einem weitgehend **ungeregelten Verfahren** betrieben. Hieraus können sich im Hinblick auf die generell „sensiblen" Datenbestände bei den Gerichten nicht unerhebliche **Sicherheitsrisiken** ergeben. Es ist deshalb auszuschließen, daß die Projektverantwortlichen noch im laufenden Echtbetrieb die technischen und organisatorischen Rahmenbedingungen modifizieren werden, weil allem Anschein nach die **Testphase** längst nicht abgeschlossen, sondern nur auf weitere Gerichte **ausgedehnt** worden ist.



Was ist zu tun?
Der Sicherheitsstandard von MEGA muß weiter verbessert werden.

4.4.2 MESTA

Kaum ist die Rechtsgrundlage für das staatsanwaltschaftliche Informationssystem GAST geschaffen worden, arbeitet das Justizministerium bereits an dem Nachfolgesystem MESTA.

Das bereits seit 1983 im Einsatz befindliche System GAST genügt offenbar nicht mehr den Anforderungen. Deshalb hat sich das Justizministerium entschlossen, gemeinsam mit den Ländern Brandenburg und Hamburg eine **Nachfolge-Software** zu entwickeln. Bereits im Sommer 1997 soll in einer Staatsanwaltschaft des Landes Schleswig-Holstein der Pilotbetrieb beginnen.

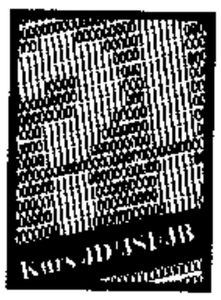
Dabei ist offenbar erkannt worden, welche Bedeutung dem Datenschutz bei einem Projekt dieser Größenordnung zukommt. Das Justizministerium hat uns von Beginn der Softwareentwicklung an über das Konzept informiert. Darüber hinaus gehört der Lenkungsgruppe als beratendes Mitglied ein Vertreter des Hamburgischen Datenschutzbeauftragten an.

Schon anhand des **Datenmodells** wurde klar, daß das Programm MESTA von seinem Datenvolumen und seiner Funktionalität her weit über GAST hinausgehen soll. Als wesentlicher Aspekt kommt hinzu, daß die Bearbeitung der Vorgänge technikgestützt erfolgen soll. Zwar wird die papierene Akte auf absehbare Zeit nicht aus dem Büro des Staatsanwaltes verschwinden, sie soll jedoch durch einen Datensatz ergänzt werden, der die Eingabe immer wiederkehrender standardisierter Informationen und den Abruf dieser Informationen erleichtert. So sollen z.B. künftig auch sämtliche zu einem Verfahren auftretende Zeugen, Sachverständige oder sonstige Verfahrensbeteiligte gespeichert werden.

Stichwort: MESTA
*MESTA ist die Abkürzung für **M**ehrländer-**S**taatsanwaltschafts-**A**utomation. Zu diesem Projekt hatten sich ursprünglich die Länder Brandenburg, Hamburg und Schleswig-Holstein zusammengefunden und der Datenzentrale Schleswig-Holstein den Auftrag zur Entwicklung des Programms gegeben. Nachträglich ist noch das Land Hessen dem Vertrag beigetreten. Oberstes Leitungsgremium des Projektes ist die sogenannte Lenkungsgruppe. Ihr gehören je ein Vertreter der vier Landesjustizverwaltungen und der Datenzentrale an. Den Datenschutzbeauftragten der beteiligten Länder wurde ein Sitz mit beratender Funktion zur Verfügung gestellt.*

Es wird also besonders wichtig sein, genau zu definieren, welche **Zugriffsrechte** auf einzelne Datensätze bestehen sollen. Ein zentraler landesweiter Zugriff darf aufgrund des zu GAST erlassenen Landesgesetzes nur auf die Beschuldigtendaten möglich sein. Einen landesweiten Zugriff auf Daten anderer Personen, wie z.B. Zeugen, darf es nicht geben.

Allerdings ist noch nicht abschließend geklärt, welche Zugriffsbeschränkungen tatsächlich bestehen werden. Das Justizministerium begründet dies damit, daß in den einzelnen am Vertrag beteiligten Ländern unterschiedliche Vorstellungen über den Umfang des Zugriffs bestünden. Das derzeitige Modell stelle eine Art **Maximalkonzept** dar, das sich bei Installation in den Staatsanwaltschaften des Landes Schleswig-Holstein auf die dort geltende Rechtslage einstellen lasse.



Schließlich bietet das neue System auch das Potential zu **datenschutzfreundlichen Verfahren**, die in GAST wegen der dort gegebenen technischen Grenzen des Verfahrens nicht realisierbar waren. So wird es jetzt technisch kein Problem sein, sämtliche Zugriffe auf den Datenbestand in einer Form zu protokollieren, die eine einfache Auswertung zu Kontroll-

zwecken ermöglicht. Da die Verschlüsselung bei Datenübertragungen immer preiswerter wird, wird man dies auch bei dem Verfahrens MESTA ins Auge fassen müssen.

Was ist zu tun?
Das Justizministerium sollte rechtzeitig ein Konzept erarbeiten, aus dem die Zugriffsbefugnisse bei dem Betrieb von MESTA in Schleswig-Holstein hervorgehen.

4.4.3 Was der Staatsanwalt der Presse mitteilen darf

Die Berichte der Medien über strafrechtliche Ermittlungsverfahren erfüllen für die Information der Öffentlichkeit eine wichtige Aufgabe. Die Informationspflicht der Staatsanwaltschaft findet aber im Persönlichkeitsrecht der Betroffenen ihre Grenze. Immerhin bedeutet Ermittlung nicht schon Anklage und schon gar nicht Verurteilung.

In der Presse finden sich täglich Berichte über Ermittlungsverfahren der Staatsanwaltschaften. Häufig werden dabei die Namen bzw. die Namenskürzel der Betroffenen genannt.

Deshalb hatte sich ein Petent an uns gewandt, als er in einer Zeitung einen Bericht über eine **Hausdurchsuchung** in seiner Wohnung las. Er war nicht nur namentlich und unter Angabe seines Alters genannt worden, überdies mußte er feststellen, daß der Artikel sogar **detaillierte Angaben** über die Ausstattung seiner Wohnung und über die dort von ihm gesammelten, privaten Gegenstände enthielt. Da bei der fraglichen Durchsuchung lediglich drei Polizeibeamte und der zuständige Staatsanwalt anwesend waren, ging der Petent davon aus, einer von ihnen habe die Informationen weitergegeben.

Die datenschutzrechtliche Bewertung des Falles muß das Spannungsfeld zwischen der grundgesetzlich garantierten Pressefreiheit und dem Grundrecht auf Datenschutz berücksichtigen. Eine lebendige Demokratie setzt voraus, daß sich die Bürger frei über wichtige Ereignisse und Entwicklungen informieren können. Die Presse erfüllt gerade mit ihrer Berichterstattung über Justizverfahren eine wichtige öffentliche Aufgabe. Diese besondere Stellung ist der Grund dafür, daß der Presse im Landespressegesetz ein Informationsrecht gegenüber staatlichen Behörden gewährt wird.

Im Wortlaut:
§ 4 Landespressegesetz
(1) Die Behörden sind verpflichtet, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen.
(2) Auskünfte können verweigert werden, soweit (...)
3. ein überwiegendes öffentliches Interesse oder ein schutzwürdiges privates Interesse verletzt würde (...)

Die **Pressefreiheit** muß jedoch mit anderen Grundrechten in Einklang gebracht werden. Die Berichterstattung über bestimmte, namentlich genannte Personen berührt deren verfassungsrechtlich garantiertes **allgemeines Persönlichkeitsrecht.**

Nach den „Richtlinien für die Zusammenarbeit der Justizbehörden mit den Medien", die das Justizministerium des Landes Schleswig-Holstein erarbeitet hat, darf deshalb im Regelfall der Name von Verfahrensbeteiligten ohne deren Zustimmung nicht genannt werden.

Auf unsere Nachfrage räumte die zuständige Staatsanwaltschaft zwar ein, daß es zu dem Ermittlungsverfahren gegen den Petenten Äußerungen gegenüber der Presse gegeben habe. Dabei seien jedoch lediglich der Name des Petenten sowie der gegen ihn erhobene strafrechtliche Vorwurf genannt worden. Dies sei rechtens, da die Presse selbst die Staatsanwaltschaft über die dem Ermittlungsverfahren zugrundeliegenden Vorwürfe informiert habe. Ihr sei daher von vornherein der Name des Petenten bekannt gewesen. Vor allem aber handele es sich bei dem Petenten um eine Person des öffentlichen Interesses, da die ihm vorgeworfenen Straftaten im Zusammenhang mit seiner Tätigkeit als Kreisvorsitzender einer politischen Partei stünden.

Die von dem Petenten vor allem beanstandeten Angaben über Details zu der Ausstattung und Größe seiner Wohnung seien jedoch nicht von der Staatsanwaltschaft an die Presse weitergegeben worden. Auch weitere Nachprüfungen bei den beteiligten Polizeibeamten konnten nicht klären, wer der Presse die fraglichen Informationen gegeben hatte.

Die Nennung des Namens des Petenten und der gegen ihn erhobenen Vorwürfe konnte in diesem konkreten Fall zwar nicht beanstandet werden, unbefriedigend blieb aber, daß die Herkunft der darüber hinausgehenden Informationen weder anhand der Akten noch gesprächsweise geklärt werden konnte.

Was ist zu tun?

Die Strafverfolgungsbehörden müssen die Richtlinien des Justizministers bei der Unterrichtung der Presse genau einhalten, weil die Folgen einer Verletzung für den Betroffenen erheblich sein können.

4.4.4 Wen schützt eigentlich das Patientengeheimnis?

Das Patientengeheimnis schützt nicht den behandelnden Arzt davor, daß seine Behandlungsmethoden mit Zustimmung des Patienten von vorgesetzten Stellen überprüft werden.

Anlaß zu dieser Feststellung gab die Eingabe eines Arztes, der in einer Justizvollzugsanstalt tätig ist. Er bemängelte das dort gebräuchliche **Formular** zur Entbindung von der ärztlichen Schweigepflicht. Mit ihrer Unterschrift können sich die Gefangenen damit einverstanden erklären, daß die behandelnden Ärzte im Falle einer Beschwerde dem Justizministerium alle gewünschten Auskünfte erteilen und die entsprechenden Unterlagen vorlegen. Der Arzt führte dazu aus, regelmäßig verlange das Justizministerium, daß die gesamte Krankenakte vorgelegt werde. Dies halte er nicht für erforderlich.

Formularmäßige Einwilligungserklärungen genügen zwar häufig nicht den datenschutzrechtlichen Anforderungen. Es ist aber leicht nachzuvollziehen, daß eine ärztliche Behandlung nur dann richtig bewertet werden kann, wenn nicht derjenige, über den Beschwerde geführt wird, darüber entscheiden kann, in welchem Umfang Akten vorgelegt werden. Soweit es daher um **Beschwerden** und Eingaben **gegen** die **ärztliche Behandlung** durch den Anstaltsarzt selbst geht, wird man auch im Interesse der Strafgefangenen die Erklärung zur Entbindung von der Schweigepflicht so zu verstehen haben, daß sie sämtliche Unterlagen betrifft, die zu einer vollständigen Bewertung der ärztlichen Behandlung aus der Sicht der Beschwerdeinstanz erforderlich sind. Dies wird häufig die gesamte Krankenakte des betroffenen Gefangenen sein. Das in Frage stehende Formular war daher nicht zu beanstanden.

4.4.5 Was Gefangene über das Wachpersonal in Erfahrung bringen konnten

Wenn Beamte des Wachpersonals von Gefangenen verletzt werden, kann der Staat Schadensersatz verlangen. Dabei dürfen jedoch nicht die privaten Verhältnisse der Verletzten leichtfertig offenbart werden.

In den vergangenen Jahren haben wir immer wieder darauf hingewirkt, die Durchsetzung des informationellen Selbstbestimmungsrechtes auch für Strafgefangene zu verbessern (vgl. z.B. 16. TB, Tz. 4.3). Dabei haben wir uns stets bemüht, auch die **Belange der Bediensteten** zu berücksichtigen. Eingaben aus dem Berichtszeitraum zeigen, wie leicht sich bei unsachgemäßer Datenweitergabe Nachteile für die Bediensteten einer JVA ergeben können.

Kommt es infolge einer Verletzung zur Dienstunfähigkeit eines Bediensteten, so werden die Bezüge weitergezahlt. Ist die Dienstunfähigkeit auf fremdes Verschulden zurückzuführen, kann der Dienstherr Schadensersatz einschließlich der verauslagten Kosten der Heilbehandlung vom Schädiger verlangen.

Dabei wurde bisher so verfahren, daß dem Schädiger auch **Belege über die Schadenshöhe** zugeschickt wurden. Darunter fanden sich z.B. Arbeitsunfähigkeitsbescheinigungen des behandelnden Arztes sowie eine Abrechnung der Dienstbezüge, die während der Erkrankung an den geschädigten Bediensteten gezahlt wurden. Außerdem wurden die Arztrechnungen, die der Geschädigte bei der Beihilfestelle eingereicht hatte, beigefügt. Sie enthielten genaue Bezeichnungen der medizinischen Leistungen, aus denen auf die Erkrankung zurückgeschlossen werden konnte. Da die Rechnungen auf den geschädigten Bediensteten ausgestellt sind, enthalten sie auch den Namen und die vollständige Privatanschrift.

Hierüber beschwerten sich zu Recht mehrere JVA-Bedienstete, die von einem Gefangenen verletzt worden waren. Ihnen war es besonders unangenehm, daß gerade die Strafgefangenen, mit denen sie bereits unliebsame Erfahrungen gemacht hatten, derartig detaillierte Informationen über ihre Person erhielten. Sie befürchteten auch, daß sich ihre **private Adresse**, Informationen über die Höhe ihrer Bezüge und ihre Krankenbehandlung in der JVA unter den Gefangenen herumsprechen würden.

Der Schadensersatzanspruch muß zwar schlüssig dargelegt werden. Das bedeutet, daß die Ursache des Schadens und seine Höhe im einzelnen anzugeben ist. Es ist zu belegen, daß die Erkrankung auf die Schädigung zurückzuführen war, wie lange der Bedienstete erkrankt war, in welcher Höhe der Bedienstete während der Zeit der Erkrankung Bezüge erhalten hat und in welcher Höhe Kosten für eine Heilbehandlung angefallen sind. Es ist allerdings **nicht erforderlich**, diese **sensiblen Informationen** bereits bei der **ersten Geltendmachung** des Schadens dem Schädiger in Form von Belegen zu offenbaren. Es muß vielmehr genügen, zunächst die Schadenshöhe darzulegen. Erst im Falle einer gerichtlichen Auseinandersetzung müssen die detaillierten Rechnungen und Belege in das Verfahren eingeführt werden. Gänzlich verzichtbar ist dagegen die Offenlegung der privaten Anschrift des Geschädigten. Diese Information steht in keinem Zusammenhang mit Höhe oder Ursache des Schadens.

Mit dem Ministerium für Finanzen und Energie des Landes Schleswig-Holstein konnte Übereinstimmung dahingehend erzielt werden, daß künftig in dieser Weise verfahren wird.

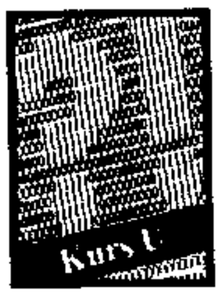
4.5 Umweltschutz - Wie lange bleiben Umweltsünden gespeichert?

Abgeschlossene Verwaltungsvorgänge dürfen nur so lange aufbewahrt werden, wie dies zur Aufgabenerfüllung erforderlich ist. Bei Kontrollen in Umweltbehörden stellte sich heraus, daß dort Informationen über Ordnungswidrigkeitenverfahren über diesen Zeitpunkt hinaus gespeichert waren.

Trotz vorhandener Vorschriften im Landesnaturschutzgesetz und der hierzu ergangenen Durchführungsvorschriften herrscht bei den Umweltbehörden offensichtlich immer noch Unsicherheit über die Aufbewahrungsfristen für personenbezogene Vorgänge. So wurden bei einer Kontrolle in einem Umweltamt seit Jahren abgeschlossene Vorgänge über **ordnungsrechtliche Maßnahmen** im Umweltbereich vorgefunden, obwohl hierfür keine Erforderlichkeit mehr vorlag. Oftmals wurden auch personenbezogene Informationen über Maßnahmen der örtlichen Ordnungsbehörden für längere Zeit gespeichert, die dem Umweltamt nur nachrichtlich zur Kenntnis gegeben worden waren.

So waren Akten über Landwirte, die vor Jahren Verstöße gegen die Vorschriften zur Güllebeseitigung begangen hatten, noch vollständig vorhanden, obwohl diese Vorgänge nach der Datenschutzverordnung zum Naturschutzgesetz schon längst hätten gelöscht sein müssen.

Auch im abfallbehördlichen Bereich, für den allerdings bisher keine bereichsspezifischen Löschungsregelungen getroffen wurden, wurden personenbezogene Vorgänge zu lange aufbewahrt. Beispielsweise erhielt das Umweltamt regelmäßig die Durchschriften der polizeilichen Anzeigen über **illegale Abfallbeseitigung** bei der zuständigen örtlichen Ordnungsbehörde zur Kenntnis. Die Durchschriften mit Namen und Adressen der Umweltsünder wurden im Umweltamt ein Jahr lang aufbewahrt, obwohl selbst die Sachbearbeiter nicht wußten, warum dies notwendig sein sollte.



Wir haben dies **beanstandet** und der datenverarbeitenden Stelle geraten, eigene Aufbewahrungsfristen, die sich am Erforderlichkeitsprinzip des Landesdatenschutzgesetzes orientieren, aufzustellen.

Was ist zu tun?
Die Umweltämter sollten ihre Aufbewahrungsfristen in einheitlichen Regelungen festlegen.

4.6 Wirtschaft, Technik und Verkehr

4.6.1 Örtliche Fahrzeugregister entsprechen nicht den Vorgaben der Fahrzeugregisterverordnung

Die Fahrzeugregisterverordnung enthält klare Regelungen, wann Daten zu löschen sind. Diese Vorgaben werden in der Praxis immer wieder verletzt. Die eingesetzten EDV-Verfahren unterstützen die gesetzlichen Löschungsfristen noch nicht.

Die Fahrzeugregisterverordnung verlangt, daß die Daten des Vorbesitzers eines Fahrzeuges ein Jahr nach Verkauf des Fahrzeuges zu löschen sind. Obwohl relativ **neue EDV-Verfahren** eingesetzt werden, ergaben Prüfungen bei zwei Zulassungsstellen, daß in den eingesetzten EDV-Programmen diese **Löschungsregelungen nicht berücksichtigt** waren. Bei der Programmerstellung wurden offenbar die bestehenden Rechtsgrundlagen nicht berücksichtigt. Die Zulassungsstellen hatten diese Programme gekauft, ohne sich vorher davon zu überzeugen, daß diese gesetzlichen Bestimmungen eingearbeitet waren. Dies haben wir beanstandet. Die Behörden müssen nun aufwendige Nachbesserungen an ihrer Software durchführen lassen.

Auch die **Aktenhaltung** bot Anlaß zu Beanstandungen. Abgeschlossene Verwaltungsvorgänge (z.B. Stillegungsverfahren wegen fehlender Versicherung oder Kfz-Steuerschulden) wurden nicht entfernt und somit mehr als die für die Fahrzeugüberwachung unbedingt erforderlichen Informationen in der Zulassungsakte gespeichert. Zwar existieren für diesen Bereich keine bereichsspezifischen gesetzlichen Löschungsvorschriften, auf der Grundlage der Regelungen im LDSG war die zeitlich unbegrenzte Aufbewahrung nicht mehr erforderlicher Vorgänge in den Zulassungsakten jedoch zu **beanstanden**.

Die Kraftfahrzeug-Zulassungsbehörden versuchen, **in Amtshilfe** für das Finanzamt fällige **Kraftfahrzeug-Steuerschulden beizutreiben**, wozu sie nach dem Kraftfahrzeug-Steuergesetz grundsätzlich verpflichtet sind. Wir sind allerdings der Auffassung, daß die festgestellte Praxis, nach fruchtlosem ersten Beitreibungsversuch des Finanzamtes sofort die Polizei mit der Entstempelung des Fahrzeuges zu beauftragen und damit also personenbezogene Daten eines Kfz-Halters an die Polizei zu übermitteln, datenschutzrechtlich zu beanstanden ist. Zunächst muß die Kfz-Zulassungsbehörde auf der Grundlage des Landesverwaltungsgesetzes versuchen, durch mildere ihr zur Verfügung stehende Zwangsmittel die Zahlung der Kraftfahrzeug-Steuerschulden herbeizuführen. Erst wenn dies scheitert und sie keine eigenen Vollstreckungskräfte hat, kommt die Beteiligung der Polizei und damit die Übermittlung personenbezogener Daten in Betracht. Im übrigen haben wir darauf verwiesen, daß die Finanzämter berechtigt sind, mit eigenen Vollstreckungskräften Fahrzeuge von Kraftfahrzeug-Steuerschuldnern stillzulegen.

Was ist zu tun?
Die Zulassungsstellen sollten ihre EDV-Verfahren an die Datenverarbeitungsbestimmungen der Fahrzeugregisterverordnung anpassen und die Zulassungsakten bereinigen.

4.6.2 Einführung des zentralen Fahrerlaubnisregisters scheint beschlossene Sache

Die Bundesregierung hat jetzt ihren Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes vorgelegt. Trotz der Bedenken der Landesbeauftragten für den Datenschutz soll ein zentrales Fahrerlaubnisregister für ca. 50 Millionen Führerscheininhaber beim Kraftfahrt-Bundesamt in Flensburg eingerichtet werden.

In unserem letzten Tätigkeitsbericht (vgl. Tz. 4.6.3) hatten wir auf die Absicht des Bundes verwiesen, das Straßenverkehrsrecht zu ändern. Der Gesetzentwurf der Bundesregierung liegt nunmehr vor. Er enthält datenschutzrechtlich problematische Bestimmungen.

Gegen die Bedenken der Datenschutzbeauftragten soll ein **zentrales Fahrerlaubnisregister** in Flensburg eingerichtet werden. Die örtlichen Fahrerlaubnisregister sollen aufgelöst werden. Dabei soll eine Bestandsbereinigung vor Übernahme der Datenbestände in das neue zentrale Register nicht erfolgen, obwohl gerade die örtlichen Fahrerlaubnisregister in vielen Bereichen inaktuell sind. Man hofft, daß durch **intensive Meldepflichten** anderer Behörden eine allmähliche Bereinigung erfolgt. So sollen z.B. **Namensänderungen** (Heirat, Adoption, Scheidung usw.) ohne vorherige Prüfung, ob die betreffende Person überhaupt im Besitz einer Fahrerlaubnis ist, an das zentrale Register gemeldet werden. Stellt sich dort beim Abgleich heraus, daß ein Eintrag vorhanden ist, wird dieser korrigiert bzw. ergänzt. Betrifft die Meldung keinen Führerscheininhaber, soll die Information sofort vernichtet werden. Auch sollen Einträge gelöscht werden, wenn eine amtliche Mitteilung über den Tod eingeht. Wer den Todesfall melden soll, läßt das Gesetz jedoch ungeregelt.

Unseren Vorbehalten gegen dieses neue zentrale Register hält die Bundesregierung entgegen, daß dieses Register **ohne aktuelle Anschrift** der Betroffenen geführt werden und nur zu den im Gesetz genannten Zwecken eingesetzt werden soll. Ob es dabei bleibt, erscheint schon deshalb fraglich, weil die örtlichen Führerscheinstellen aufgelöst werden sollen und die dort zusätzlich gespeicherten Daten vermutlich in das zentrale Register überführt werden.

Auch die Halterdatei in Flensburg, deren Zweckbestimmung ebenfalls genau definiert ist, wird offensichtlich mehr und mehr zu einem Register, das wegen seiner Aktualität und Zentralität auch für andere Zwecke genutzt wird. So sollen demnächst **unterhaltspflichtige Väter**, die ihrer Unterhaltspflicht nicht nachkommen und deren Aufenthaltsort unbekannt ist, mit Hilfe der Eintragung im Kraftfahrzeugregister **aufgespürt** werden. Dies liege im öffentlichen Interesse, da die öffentlichen Kassen durch die Heranziehung der aufgespürten Unterhaltssäumigen entlastet würden. Nicht daß die Suche nach zahlungsunwilligen Vätern nicht wichtig und im öffentlichen Interesse wäre. Aber sie hat mit der Kfz-Zulassung nichts zu tun. Welche Begehrlichkeiten werden über kurz oder lang angesichts der zentralen Speicherung von mindestens 50 Millionen Bundesbürgern im zentralen Fahrerlaubnisregister entstehen?

Weiter ist zu bemängeln, daß die ursprünglich ausschließlich für Zwecke des Datenschutzes und zur Aufdeckung mißbräuchlicher Anfragen geführten **Aufzeichnungen automatisierter Abrufe** aus den zentralen Registern nunmehr darüber hinaus für Strafverfolgungszwecke verwendet werden sollen. Auch in diesem Falle wird eine bei der Einführung des Datenbestandes besonders betonte Zweckbindung über Bord geworfen, weil einmal vorhandene Daten für andere Zwecke nützlich zu sein scheinen.

Wenigstens sieht der Gesetzentwurf erstmalig **Löschungsfristen** für Akteninhalte vor. Auch die restriktive Regelung der Verwendung von Registerauskünften, Führungszeugnissen, Gutachten und Gesundheitszeugnissen ist positiv zu bewerten.

Was ist zu tun?
Bundesrat und Bundestag sollten die Notwendigkeit der Einführung eines neuen zentralen Registers sorgfältig prüfen.

4.6.3 Wenn der Bürger seine Unschuld beweisen muß

Belastende Informationen, die eine Behörde für künftige Nutzungen speichert, müssen immer auf dem aktuellen Stand gehalten werden. Sind Daten als vorläufig gekennzeichnet, so muß ihre Richtigkeit überprüft werden, bevor Maßnahmen zu Lasten des Bürgers getroffen werden.

Wie sich die Dinge gleichen: Erneut ist von einem Fall zu berichten, in dem die Fahrerlaubnisbehörde nur über die Information verfügte, daß ein **Führerschein vorläufig beschlagnahmt** worden war (vgl. 17. TB, Tz. 4.6.1). Tatsächlich hatte auch in dem neuerlichen Fall das Gericht den Betroffenen freigesprochen und ihm den Führerschein wieder ausgehändigt. In beiden Fällen versäumte es jedoch das Gericht, den Fahrerlaub-

nisbehörden diesen Umstand mitzuteilen.

Als der Betroffene seinen Führerschein verlor und einen neuen beantragte, stellte sich die Behörde stur. Auch nachdem sie selbst aus dem Verkehrszentralregister die Mitteilung erhalten hatte, daß keine Fahrerlaubnisentziehung gespeichert war, und die Staatsanwaltschaft ihr mitgeteilt hatte, daß dort keine Akte mehr existierte, stellte sie ihm immer noch keinen Ersatzführerschein aus und beharrte auf der Vorlage von **Nachweisen seiner Unschuld**. Erst durch unsere Mithilfe und nach Vorlage des Einstellungsbeschlusses, der sich dann doch noch anfand, wurde dem Betroffenen ein Ersatzführerschein ausgestellt. Die ganze Angelegenheit zog sich jedoch über mehr als zwei Monate hin.

Wir haben die Vorgehensweise der Behörde beanstandet, weil sie auch dann noch auf der Meinung beharrte, der Führerschein sei entzogen worden, als klare Anhaltspunkte für das Gegenteil sprachen. Selbst wenn die Richtigkeit oder die Unrichtigkeit der umstrittenen Informationen weder von ihr noch vom Betroffenen hätte nachgewiesen werden können, wäre dem Petenten ein Ersatzführerschein auszustellen gewesen. Denn die umstrittenen Informationen hätten zumindest gesperrt werden müssen und hätten folglich nicht gegen den Betroffenen verwendet werden dürfen.

Das Verkehrsministerium hat sich unserer Auffassung angeschlossen und umgehend alle Fahrerlaubnisbehörden auf die bestehende Rechtslage hingewiesen.

Was ist zu tun?
Die Fahrerlaubnisbehörden müssen ihrer Pflicht, sich nach dem Ausgang eingeleiteter Verfahren zu erkundigen, nachkommen. Die Gerichte müssen ihrerseits ihre Nachberichtspflicht erfüllen.

4.6.4 Das lange Leben von Verkehrsordnungswidrigkeiten

Informationen über Verkehrsordnungswidrigkeiten, die nicht in das Verkehrszentralregister einzutragen sind, sind aus der Führerscheinakte zu entfernen, wenn der Vorgang abgeschlossen ist.

Ein Bürger hatte in den Jahren **1986** und **1987** einige Verkehrsordnungswidrigkeiten begangen, die jeweils mit Verwarnungsgeldern geahndet wurden. Seinerzeit erhob die Fahrerlaubnisbehörde Eignungsbedenken gegenüber dem Betroffenen und ordnete die Entziehung seiner Fahrerlaubnis an. Das Verwaltungsgericht war jedoch anderer Rechtsauffassung und erklärte die Entziehung für unzulässig, weil „Verkehrsverstöße, die im Verwarnungsverfahren gerügt werden können, grundsätzlich bei der Prüfung der Eignung eines Kraftfahrers unberücksichtigt bleiben“. Dies

hinderte die Fahrerlaubnisbehörde nicht, die Informationen zehn Jahre lang zu speichern. Wir haben die **Speicherung beanstandet**, weil die Aufbewahrung dieser alten Vorgänge zur Aufgabenerfüllung der Fahrerlaubnisbehörde nicht mehr erforderlich war und diese somit nach den Vorschriften des Landesdatenschutzgesetzes zu löschen waren.

Was ist zu tun?
Die Fahrerlaubnisbehörden sollten entsprechend dem Erlaß des Verkehrsministeriums aus dem Jahre 1995 ihre Akten bereinigen.

4.7 Sozialwesen

4.7.1 Ein Federstrich des Gesetzgebers - Datenschutz für Sozialhilfeempfänger hat keine Konjunktur

Durch eine Änderung des Bundessozialhilfegesetzes in letzter Minute im Vermittlungsausschuß ist es den Sozialämtern nunmehr erlaubt, die Daten der Sozialhilfeempfänger mit anderen Dateien abzugleichen. Der Kritik der Datenschutzbeauftragten an bisherigen Abgleichen wurde dadurch der Wind aus den Segeln genommen.

Im 18. Tätigkeitsbericht wurde unter Tz. 4.7.1 darüber berichtet, daß ein Sozialamt unter Umgehung der gesetzlichen Bestimmungen die Kraftfahrzeugdaten sämtlicher Sozialhilfeempfänger mit den Daten der Kraftfahrzeug-Zulassungsstelle abgeglichen hatte. Zum Zeitpunkt der Prüfung war dieser Totalabgleich unzulässig. Das Sozialamt hätte nur bei Vorliegen konkreter Anhaltspunkte bei der Zulassungsstelle nachfragen dürfen, ob der Betroffene Halter eines Pkw ist. In dem konkreten Fall wurde daher die Übermittlung der Daten von 4500 Hilfeempfängern durch das Sozialamt an die Zulassungsstelle als rechtswidrig gewertet und beanstandet.

Inzwischen hat der Gesetzgeber im Rahmen des Gesetzes zur Reform des Sozialhilferechts eine ergänzende Vorschrift geschaffen, die künftig einen **automatisierten Datenabgleich erlaubt**. Sie wurde in letzter Minute durch den Vermittlungsausschuß eingefügt.

Die Tatsache, daß der Gesetzgeber hier Handlungsbedarf für eine entsprechende Regelung gesehen hat, zeigt eindeutig, daß die bisherigen Vorschriften des Bundessozialhilfegesetzes nicht als ausreichende Rechtsgrundlage für einen umfassenden automatisierten Abgleich angesehen werden konnten - ein schwacher Trost.

Was ist zu tun?
Das neue Gesetz läßt den Datenabgleich zu, schreibt ihn aber nicht zwingend vor. Die Sozialämter müssen entscheiden, ob sie davon Gebrauch machen wollen.

4.7.2 Was Sozialhilfeempfängern zugemutet wird

Beleidigende Sprüche an der Pinnwand des Sachbearbeiters zeigen, mit welcher Einstellung dort den Sozialhilfeempfängern begegnet wurde.

Aufgrund eines Antrags der Tochter auf Sozialhilfe sollte eine Mutter Angaben zu ihren Einkommens- und Vermögensverhältnissen machen. Sie besuchte aus diesem Grund das örtliche Sozialamt und war schokkiert. An der Wand gegenüber dem Besucherstuhl im Büro des Sachbearbeiters hing an einer Pinnwand folgender Text:

„Gerade entlassen? aus dem Irrenhaus?
aus dem Gefängnis?
aus dem Aufsichtsrat?
Sie denken bereits daran,
Tante Olga zu entführen?
eine Bank auszurauben?
eine Arbeit anzunehmen?
Wir haben die bessere Idee!

Sozialhilfe
mit dem geilen Wohngeld
Kommen Sie zu uns! **Volle Knete ohne**
Plackerei

Ihr Team vom Sozialamt
Auskunft erteilt
Herr XYZ“
(hier stand der Name des zuständigen Sachbearbeiters)

Die Betroffene hat sich empört über diesen Text an uns gewandt. Sie erklärte, sie sei nicht bereit, einem Amt, in dem die Hilfesuchenden zutiefst verletzt und verhöhnt werden, Auskünfte zu erteilen. Auf unsere Intervention hin wurde der besagte Text entfernt und der Mitarbeiter ermahnt.

Obwohl es hier nicht um datenschutzrechtliche Regelungen ging, hatte die Petentin recht mit ihrem Gefühl, daß Grundvoraussetzung für den Umgang mit dem Bürger und damit auch für jede faire Datenerhebung die Achtung und der Respekt vor dem Menschen sein muß. Nur dann kann vom Bürger verlangt werden, daß er der Behörde auch sensible Daten offenbart.

4.7.3 Der Vermieter muß nicht alles wissen

Die Wohngeldstelle muß die Daten, die zur Bearbeitung eines Wohngeldantrages notwendig sind, grundsätzlich beim Betroffenen erheben. Der Vermieter muß von dem Vorgang keine Kenntnis bekommen, wenn der Mieter die notwendigen Angaben selbst machen kann.

Eine Petentin beschwerte sich darüber, daß die Wohngeldstellen bei Wohngeldanträgen bestimmte Daten durch die Mieter mit einem Vordruck beim Vermieter erheben lassen. Das Formular ist mit folgendem Text überschrieben: „Zur Vorlage bei der Wohngeldstelle", enthält den Namen des Mieters und ist häufig mit dem Hinweis auf die Strafbarkeit unrichtiger Angaben versehen.

Es wird der Eindruck erweckt, die Angaben müßten immer beim Vermieter eingeholt werden. Dies widerspricht aber dem Grundsatz, daß Sozialdaten **vorrangig beim Betroffenen** zu erheben sind. Antragsteller sollen selbst darüber entscheiden, wer erfährt, daß sie Wohngeld beantragt haben. Der beschriebene Vordruck läßt nicht erkennen, daß der Betroffene eine **Wahlmöglichkeit** hat, denn erforderlich ist die Einschaltung des Vermieters nur, wenn der Mieter die erforderlichen Angaben für die Wohngeldberechnung nicht selbst machen und belegen kann.

Der Innenminister teilt unsere Auffassung und hat die Wohngeldstellen darauf hingewiesen, daß sie dem Antragsteller die Möglichkeit einzuräumen haben, alle notwendigen Angaben selbst zu erbringen.

Was ist zu tun?
Die Wohngeldstellen müssen den Hinweis des Innenministers beachten und Wohngeldantragsteller darauf aufmerksam machen, daß es ihnen freigestellt ist, die notwendigen Informationen selbst zu geben oder beim Vermieter einzuholen.

4.7.4 Schwierige Abwägung bei der Akteneinsicht

Auch in Sorgerechtsfällen besteht ein Akteneinsichtsrecht. Allerdings müssen die Belange der Betroffenen sorgfältig abgewogen werden. Die Jugendämter müssen die Namen von Informanten nicht preisgeben, es sei denn, es liegen Anhaltspunkte für eine vorsätzliche oder fahrlässige Falschinformation vor.

Im Rahmen der Auseinandersetzungen um das Sorgerecht für die gemeinsame Tochter hatte ein Vater Akteneinsicht in die Akten des Allgemeinen Sozialdienstes beim Jugendamt beantragt. Die Ehefrau hatte

der Einsichtnahme in die betreffenden Aktenteile nicht zugestimmt. Als der Kreis sich an uns wandte, wiesen wir auf folgendes hin:

In solchen Fällen kann die Lösung nur im Rahmen einer **Güterabwägung** gefunden werden, um dem Spannungsfeld zwischen den Interessen der Beteiligten oder Dritten und dem Recht des Betroffenen auf Akteneinsicht gerecht zu werden. Das Recht auf Akteneinsicht darf allerdings nur in dem Umfang beschränkt werden, wie die berechtigten Interessen dies erfordern, so daß in der Regel zumindest eine Teileinsicht zu gewähren ist. Es ist jeweils bezogen auf das einzelne Schriftstück zu prüfen, ob die Auskunftserteilung gegen die berechtigten Interessen der Dritten verstößt. Wir haben den Kreis gebeten, unter Berücksichtigung dieser Aspekte eine Entscheidung zu treffen.

Im Wortlaut: § 25 Abs. 1 u. 3 SGB X

(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Satz 1 gilt bis zum Abschluß des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung.

(3) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheimgehalten werden müssen.

In einem anderen Fall trennte sich die Ehefrau von ihrem Mann und verließ mit den Kindern die gemeinsame Wohnung. Sie ging in eine andere Stadt, wo sie in einem Frauenhaus Unterkunft fand. Der Vater versuchte daraufhin einen Gerichtsbeschluß gegen seine Ehefrau auf Herausgabe der beiden Kinder zu erwirken.

Das Jugendamt machte in seinem Bericht für das Gericht geltend, daß der Vater nicht in der Lage sei, verantwortlich für seine Kinder zu sorgen. Daraufhin wurde das Sorgerecht der Mutter zugesprochen. Der Vater begehrte nach dieser Entscheidung Einsicht in die Jugendamtsakte, da nach seiner Auffassung die zuständige Sachbearbeiterin in ihrem Bericht an das Gericht wahrheitswidrige Beschuldigungen Dritter berücksichtigt habe. Dies wurde abgelehnt.

Das Ergebnis unserer datenschutzrechtlichen Überprüfung lautete: Obwohl grundsätzlich ein **Auskunftsanspruch** bestand, überwog das Geheimhaltungsinteresse des Jugendamtes. Es darf Hinweise dann speichern, wenn dies erforderlich ist, um Gefährdungen des Kindeswohls abzuwehren (vgl. auch Tz. 4.7.5). Die **Zusicherung der Vertraulichkeit** kann dabei angemessen sein. Da solche Hinweise oftmals aus der Nachbarschaft oder eventuell aus dem familiären Umkreis stammen, kann es angezeigt sein, dem Informanten durch die vertrauliche Behandlung der Informationen die Möglichkeit eines weiteren friedlichen Zusammenlebens mit den betroffenen Familien zu erhalten. Die Bereitwilligkeit

potentieller Auskunftspersonen zur Zusammenarbeit würde nachlassen, wenn bekannt werden würde, daß vertrauliche Mitteilungen vom Jugendamt ohne weiteres preisgegeben werden.

Auf die Zusicherung der Vertraulichkeit kann sich allerdings nicht verlassen, wer wider besseres Wissen oder leichtfertig falsche Informationen gegeben hat. Es liegt nicht im öffentlichen Interesse, Denunzianten, die wahrheitswidrige Angaben machen, zu schützen. Im konkreten Fall waren keine Anhaltspunkte dafür gegeben, daß die Informanten wahrheitswidrige Angaben gemacht haben. Die Verweigerung der Auskunft war daher datenschutzrechtlich nicht zu beanstanden.

Was ist zu tun?
Die Jugendämter dürfen bei der Gewährung von Akteneinsicht in Sorgerechtsfällen nicht schematisch verfahren, sondern müssen die Interessen der Beteiligten sorgsam abwägen.

4.7.5 Wenn das Jugendamt im Kindergarten nachfragt

Das Jugendamt darf nur in begründeten Fällen Daten ohne Einwilligung der Betroffenen bei Dritten erheben. Private Kindergärten haben keine Auskunftspflicht. Sie dürfen Auskunft geben, wenn es im Interesse des Kindes notwendig ist, z.B. bei Verdacht auf Kindesmißhandlung.

Im Sozialdatenschutzrecht gilt der Grundsatz, daß Daten vorrangig beim Betroffenen zu erheben sind. Wenn es um Hilfeleistungen geht, können die Informationen in der Regel nur **beim Betroffenen** eingeholt werden, denn er selbst entscheidet darüber, ob er Hilfe für sich bzw. seine Familie in Anspruch nehmen möchte. Da Leistungen nicht aufgedrängt werden können, verbietet sich eine Datenerhebung hinter dem Rücken der Betroffenen. Vor allem birgt aber eine heimliche Datenerhebung die Gefahr in sich, daß die Betroffenen sich hintergangen fühlen und nicht mehr bereit sind, mit dem Jugendamt zusammenzuarbeiten.

Stichwort:
Kinder- und Jugendhilfegesetz
Das Kinder- und Jugendhilfegesetz sieht im wesentlichen zwei Aufgabenbereiche des Jugendamtes vor. Den Bereich der Leistungsverwaltung und den der Eingriffsverwaltung. Die Eltern haben einen Anspruch auf Hilfen, die sie, wenn sie wollen, in Anspruch nehmen können, so z.B. Hilfen zur Erziehung. Wenn aber eine Gefahr für das Wohl des Kindes besteht und die Eltern zu Auskünften nicht bereit sind, ist das Vormundschaftsgericht zum Schutz der Kinder anzurufen. Sofern sich die Kinder nicht in der Obhut der Eltern befinden, können auch Informationen bei Dritten erhoben werden.

Was aber kann das Jugendamt unternehmen, wenn es befürchtet, daß das Wohl des Kindes gefährdet ist und die Eltern nicht bereit sind, die Situation für das Kind zu ändern? Kann es dann z.B. bei privaten Kindergärten Informationen einholen, und sind die Kindergärten zu einer Antwort verpflichtet? Eine Datenerhebung bei Dritten kommt nur in Betracht, wenn das Kind oder der Jugendliche sich nicht in der **Obhut der Eltern** befindet, also z.B. von zu Hause ausgerissen ist. Ansonsten hat das Jugendamt durch die Kontaktaufnahme mit den Eltern zu klären, ob das Wohl des Kindes gefährdet ist. Erhärtet sich dabei der Verdacht, daß z.B. das Kind mißhandelt wird, so hat das Jugendamt das Vormundschaftsgericht anzurufen.

In den Fällen, in denen das Jugendamt die Daten bei Dritten erheben darf und dies auch erforderlich ist, darf es z.B. auch im Kindergarten nachfragen. Die Verantwortlichen im Kindergarten müssen dann selbst entscheiden, ob sie über das Kind Auskunft geben. Es ist ihnen erlaubt, wenn es im Interesse des Kindes oder der Allgemeinheit liegt. Davon ist bei **Verdacht auf Kindesmißhandlung** regelmäßig auszugehen.

Was ist zu tun?
Jugendämter müssen zunächst immer versuchen, mit den Eltern Kontakt aufzunehmen.

4.7.6 Verarbeitung von Versichertendaten im Auftrag

Die Kontrolle einer Krankenkasse förderte Mängel bei der Gestaltung der Auftragsdatenverarbeitung zutage.

Bei der Überprüfung der Arbeitsabläufe in einer Krankenkasse ergab sich, daß man sich eines Rechenzentrums in Nordrhein-Westfalen bediente. Für eine derartige Verarbeitung von Versichertendaten gelten die besonderen Bestimmungen des Sozialgesetzbuches für die Verarbeitung von Sozialdaten im Auftrag. Diese wurden von der geprüften Kasse allerdings nicht eingehalten:

- Es war versäumt worden, dieses Auftragsverhältnis rechtzeitig dem Sozialministerium anzuzeigen.
- Der geschlossene **Vertrag** trug nicht der Tatsache Rechnung, daß für die Einhaltung der Datenschutzvorschriften die schleswig-holsteinische Krankenkasse verantwortlich bleibt. Es fehlten z.B. Vereinbarungen über die technischen und organisatorischen Maßnahmen zur Datensicherheit. Der Vertrag enthielt nur die allgemeine Klausel: „Das Rechenzentrum wird bei der nach diesem Vertrag auftragsweise durchzuführenden Datenverarbeitung die Bestimmungen für den Datenschutz und Datensicherung berücksichtigen".

Bislang hat die Krankenkasse die Mängel in der Vertragsgestaltung noch nicht beseitigt.

4.8 Gesundheitswesen

4.8.1 Das schleswig-holsteinische Krebsregistergesetz

Das schleswig-holsteinische Krebsregistergesetz strebt eine möglichst hohe Meldequote an. Deshalb ist eine Meldepflicht für Ärzte vorgesehen. Die datenschutzrechtlichen Belange der Patienten sollen durch Anonymisierung gewahrt werden.

Epidemiologische Forschung kann einen sinnvollen und wichtigen Beitrag leisten, wenn es um die **Bekämpfung von Krebserkrankungen** geht. Um ein Netz von epidemiologischen Krebsregistern auf Länderebene aufzubauen, wurde vom Bundesgesetzgeber das Krebsregistergesetz erlassen, das die Länder verpflichtet, **Krebsregister** einzurichten. Hierbei wurden den Ländern bei der Ausgestaltung der Vorgehensweise Freiräume gelassen, die durch Ausführungsgesetze genutzt werden können. Scheswig-Holstein hat als erstes Bundesland ein solches Gesetz erlassen und inzwischen mit dem konkreten Aufbau des Registers begonnen.

> ***Stichwort:***
> ***Epidemiologische Forschung***
> *Lehre von den Verteilungen der Krankheiten, den Bedingungen, die bei ihrer Entstehung von Bedeutung sind, sowie von den wirtschaftlichen, sozialen und psychischen Folgen der Erkrankungen. Ein wesentliches Ziel ist die Bereitstellung von Daten für die Planung und Durchführung von Maßnahmen zur Vorbeugung und Bekämpfung von Krankheiten.*

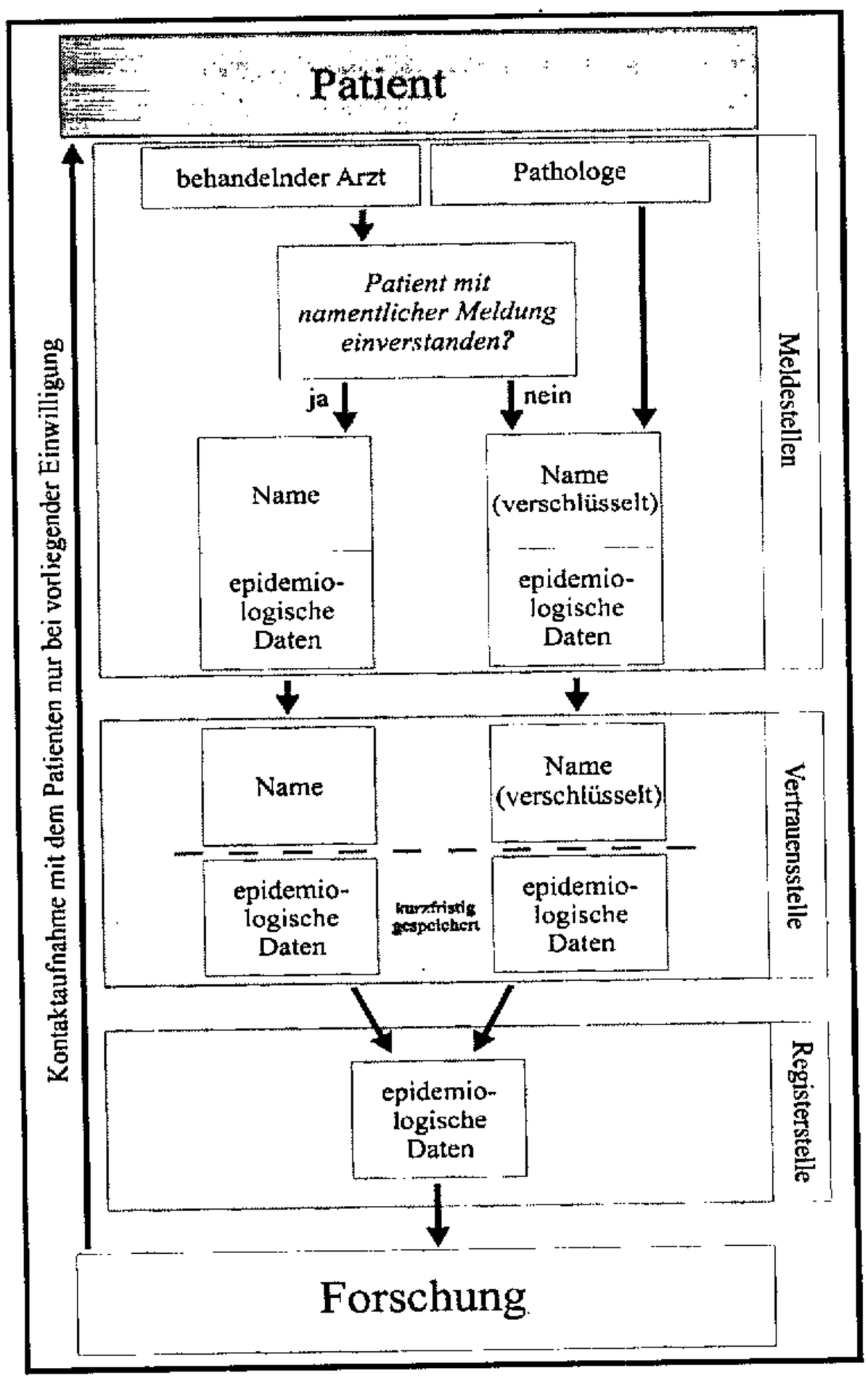
Das Land hatte die Absicht, eine möglichst vollständige Erfassung aller Krebserkrankungen zu erreichen, um eine effektive epidemiologische Forschung zu gewährleisten. Aus diesem Grund wurde in Schleswig-Holstein den Ärzten eine **Meldepflicht** auferlegt. Das Vollständigkeitsprinzip bedeutet auch, daß die epidemiologischen Daten selbst von solchen erkrankten Personen in das Krebsregister aufgenommen werden müssen, die entweder über ihre Krebserkrankung gar nicht informiert wurden oder die nach einer Information durch ihren Arzt ihre namentliche Speicherung im Krebsregister ablehnen. Um zu vermeiden, daß Erkrankte ohne Einwilligung namentlich erfaßt werden, ist vorgesehen, den Namen schon bei den meldenden Ärzten zu verschlüsseln (**periphere Informationsreduktion**). Dadurch sind die betroffenen Personen davor geschützt, daß die Mitarbeiter des Krebsregisters ihren Namen erfahren oder daß sich Dritte im Rahmen von Forschungsvorhaben unmittelbar an sie wenden können.

Das Meldeverfahren ist insofern **grundrechtsfreundlich** ausgestaltet, denn die Betroffenen müssen nicht von sich aus initiativ werden, wenn sie nur anonym gespeichert werden wollen. Sie müssen nur mit Nein antworten, wenn sie gefragt werden, ob sie mit einer namentlichen Speicherung einverstanden sind bzw. ob sie eine Forschung mit personenbezogenen Daten erlauben.

Die **Qualität der Verschlüsselung** im Rahmen des schleswig-holsteinischen Krebsregisters für das Grundrecht auf informationelle Selbstbestimmung von ganz besonderer Bedeutung. Da jedoch auch eine Namensverschlüsselung nicht in allen Fällen einen 100%igen Schutz vor einer Deanonymisierung bieten kann, haben wir darauf hingewirkt, daß die Registerstelle keine Datensätze an Dritte übermitteln darf, wenn ein **Deanonymisierungsrisiko** besteht. Auch eine Reihe weiterer Vorschläge, die einen möglichst optimalen Schutz des Patientengeheimnisses gewährleisten sollen, wurden in das Gesetz übernommen.

Wir werden die Einrichtung des Krebsregisters weiterhin aufmerksam mitverfolgen. Sollten sich bei der Umsetzung des Gesetzes Schwachstellen für den Grundrechtsschutz der Bürgerinnen und Bürger zeigen, werden wir uns für Abhilfe einsetzen.

Wie die **Meldewege** im einzelnen aussehen, soll die nachfolgende Übersicht veranschaulichen:



4.8.2 Universitätskliniken bitten künftig Patienten bei Forschung um Einwilligung

Die Forschung mit Patientendaten darf nur im Rahmen der sogenannten Eigenforschung bzw. mit anonymen Daten erfolgen oder wenn eine Einwilligung des Patienten vorliegt. Die Universitätskliniken reagieren auf unsere Kritik.

Im Rahmen einer Prüfung in einer Universitätsklinik hatte sich herausgestellt, daß Patientenakten **ohne Einwilligung** der Betroffenen nach der Behandlung in nicht anonymisierter Form **für Forschungszwecke verwendet** werden (vgl. 17. TB, Tz. 6.2.2, 18. TB, Tz. 6.7.2). Dies wurde als unzulässig beanstandet, da die Forschung mit Patientendaten nach dem Landesdatenschutzgesetz und der ärztlichen Berufsordnung nur

Stichwort: Ärztliche Schweigepflicht
Die im Eid des Hippokrates enthaltene Schweigepflicht der Ärzte dürfte die älteste bereichsspezifische Datenschutzvorschrift überhaupt sein. In der Berufsordnung der Ärzte ist ausdrücklich festgeschrieben, daß Patientendaten zu Forschungszwecken nur mitgeteilt werden dürfen, wenn der Patient anonym bleibt oder er ausdrücklich zugestimmt hat. § 203 Strafgesetzbuch stellt die unbefugte Offenbarung von Patientendaten unter Strafe.

- in anonymisierter Form oder
- mit der Einwilligung der Patienten oder
- zur eigenen Forschung der behandelnden Ärzte

zulässig ist.

Die Universitätskliniken in Kiel und Lübeck wollen in Zukunft **Einwilligungserklärungen** verwenden, in denen die Patienten ausführlich über den Aspekt der Forschung informiert werden und selbst entscheiden können, ob ihre Behandlungsunterlagen für Forschungszwecke zur Verfügung stehen. Dadurch wollen sie erreichen, daß für die Durchführung von Forschungsvorhaben ausreichendes Datenmaterial zur Verfügung steht.

Darüber hinaus dürfen die behandelnden Ärzte auch ohne Einwilligung mit den Daten ihrer eigenen Patienten forschen (Eigenforschung). Notwendig ist es allerdings zu definieren, wer behandelnder Arzt ist. Zum Behandlungsteam gehören nach unserer Auffassung alle Ärzte, die den Patienten gleichzeitig oder nacheinander behandeln. Darüber hinaus gehören zum Behandlungsteam auch die direkten Funktionsnachfolger der behandelnden Ärzte.

Was ist zu tun?
Zuerst ist immer zu prüfen, ob nicht auch eine Forschung mit anonymisierten Daten möglich ist. Ansonsten ist die ausdrückliche Einwilligung der Patienten einzuholen.

4.8.3 Stichtagserhebungen des Medizinischen Dienstes

Querschnittsprüfungen des Medizinischen Dienstes der Krankenversicherung in Krankenhäusern anhand von nicht anonymisierten Patientenunterlagen sind rechtlich problematisch.

In mehreren schleswig-holsteinischen Krankenhäusern erfolgte eine **Querschnittsprüfung** (Stichtagserhebung) durch den Medizinischen Dienst der Krankenversicherung (MDK). Es wurden sämtliche Akten von Patienten geprüft, die an einem bestimmten Tag stationär behandelt worden waren.

> ***Stichwort: Medizinischer Dienst der Krankenversicherung***
> *Der Medizinische Dienst der Krankenversicherung (MDK) ist eine Körperschaft des öffentlichen Rechts, die an die Stelle des früheren vertrauensärztlichen Dienstes getreten ist. Er ist eine Arbeitsgemeinschaft der Krankenkassen, die Gutachter-, Beratungs- und Prüfungstätigkeiten ausübt. So hat der MDK u.a. die Aufgabe, bei der Feststellung der Pflegebedürftigkeit mitzuwirken, Vorschläge zur Sicherung des Heilerfolgs und zur Einleitung von Rehabilitationsmaßnahmen zu machen und Gutachten bei Zweifeln an der Arbeitsunfähigkeit zu erstatten.*

Zwar gibt es im Krankenhausfinanzierungsgesetz (KHG) eine Aufgabenzuweisung an den Medizinischen Dienst, die vorsieht, daß er zur Feststellung von Fehlbelegungen in Krankenhäusern auch Einsicht in Krankenunterlagen nehmen kann. Eine solche gesetzliche Regelung ist aber immer auch am **Grundsatz der Verhältnismäßigkeit** zu messen. Stichtagserhebungen sind sicherlich geeignet, Fehlbelegungen festzustellen, zweifelhaft ist aber, ob es erforderlich ist, daß hierzu von der Identität der Patienten Kenntnis genommen wird. Hinzu kommt, daß das Krankenhausfinanzierungsgesetz eine systematisch nicht gelungene Erweiterung der Aufgaben des Medizinischen Dienstes der Krankenversicherung enthält, die im übrigen im SGB V geregelt sind.

Ein weiteres Problem der Stichtagserhebungen in Schleswig-Holstein war, daß die Daten zur Klärung offener Strukturfragen im Rahmen der **Budgetverhandlungen** für das Jahr 1996 erhoben wurden. Es ist zweifelhaft, ob damit § 17 a Krankenhausfinanzierungsgesetz als Rechtsgrundlage überhaupt in Betracht kommt. Die Novellierung des Krankenhausfinanzierungsgesetzes diente vorrangig zwei Zwecken: zum einen der Entlastung der gesetzlichen Krankenversicherung durch den Abbau

der Fehlbelegung von Krankenhausbetten und zum anderen der Umwidmung der vom Bettenabbau betroffenen Krankenhausabteilungen in Pflegeeinrichtungen.

> ***Im Wortlaut: § 17 a Abs. 2 KHG***
> *Die Krankenkassen wirken insbesondere durch gezielte Einschaltung des Medizinischen Dienstes der Krankenversicherung darauf hin, daß Fehlbelegungen vermieden und bestehende Fehlbelegungen zügig abgebaut werden. Zu diesem Zweck darf der Medizinische Dienst der Krankenversicherung Einsicht in die Krankenunterlagen nehmen. Der Medizinische Dienst hat der Krankenkasse das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund mitzuteilen.*

Schließlich war gegenüber dem Medizinischen Dienst und den Kassen darauf hinzuweisen, daß der Medizinische Dienst allenfalls die Unterlagen von Kassenmitgliedern einsehen darf. Trotz nach wie vor bestehender Zweifel an der Erforderlichkeit und damit auch der Rechtmäßigkeit der querschnittsmäßigen Stichtagserhebungen durch den Medizinischen Dienst in personenbezogener Form werden wir diese Datenerhebungen im Hinblick auf die nicht eindeutige Rechtslage **nicht beanstanden**, weil wie folgt vorgegangen werden soll:

- In diesem Jahr wird nur eine begrenzte Zahl ausgewählter Kliniken überprüft. Am Ende des Jahres wird noch einmal über das weitere Vorgehen - auch unter Berücksichtigung der Erfahrungen in anderen Bundesländern - gesprochen.

- Bei den Stichtagserhebungen werden nur die Krankengeschichten von Versicherten der gesetzlichen Krankenkassen ausgewertet.

- In diesem Zusammenhang soll auch geprüft werden, inwieweit automatisierte Verfahren von Anfang an anonymisierte Prüfungsansätze ermöglichen.

- Außerdem wird zu prüfen sein, ob im Hinblick auf § 17 a Abs. 3 KHG, der ohnehin pauschale Budgetkürzungen wegen Fehlbelegung vorsieht, künftig Stichtagsprüfungen überhaupt noch erforderlich sind.

4.8.4 Keine Intimsphäre in der Klinik?

Die Befragung über persönliche Daten bei der Krankenhausaufnahme im Beisein anderer Patienten verstößt gegen die ärztliche Schweigepflicht, wenn der Patient nicht damit einverstanden ist.

Ein Klinikpatient schilderte uns, daß bei seiner Krankenhausaufnahme eine erste Befragung über seine persönlichen Daten wie Name, Anschrift, Telefonnummer, Vorerkrankungen, Kinderkrankheiten usw. auf dem **Krankenhausflur** in unmittelbarer Nähe zu anderen Patienten durchge-

führt wurde. Bei anderen Patienten sei ebenso verfahren worden. Darüber hinaus habe die Eingangsuntersuchung in einem 4-Bett-Zimmer im Beisein der anderen Patienten stattgefunden.

Die Klinik hat den Sachverhalt auf Anfrage bestätigt. Wir haben dies als eine **Verletzung der ärztlichen Schweigepflicht** kritisiert und Abhilfe gefordert. Die Klinik machte geltend, daß eine Befragung der Patienten in unmittelbarer Nähe anderer Patienten aufgrund der begrenzten Räumlichkeiten in der Regel unumgänglich sei. Eine Änderung sei nur durch einen Neubau zu erreichen. Trotz dieser eher ablehnenden Haltung hat dann aber doch unter Beteiligung des Landesbauamtes eine Ortsbesichtigung stattgefunden. Dabei stellte sich heraus, daß auch ein **Umbau** ausreichend war, der inzwischen vom zuständigen Ministerium **genehmigt** wurde.

Was ist zu tun?
Die Umbauarbeiten sollten so schnell wie möglich durchgeführt werden.

4.8.5 Einsicht eines Betreuers in Gesundheitsunterlagen

Eine Klinik darf einem Betreuer, dem die Gesundheitssorge für den Betreuten obliegt, nicht die Einsicht in ärztliche Entlassungsberichte verwehren. Die Fachklinik für Psychiatrie, Neurologie und Rehabilitation in Neustadt stellte sich stur und reagierte erst auf Anweisung des Ministeriums.

Für eine psychisch kranke Person war für den Bereich der Gesundheitssorge ein Betreuer bestellt worden. Nachdem die von ihm betreute Person aufgrund ihrer psychischen Erkrankung in der Klinik behandelt worden war, wollte er Einsicht in den ärztlichen Entlassungsbericht nehmen. Dies wurde ihm von der Klinik mit dem Argument verwehrt, es stelle einen Verstoß gegen die ärztliche Schweigepflicht dar.

Stichwort: Betreuung
Wenn Erwachsene aufgrund einer psychischen Krankheit oder seelischen, körperlichen bzw. geistigen Behinderung ihre Angelegenheiten ganz oder teilweise nicht mehr besorgen können, bestellt das Vormundschaftsgericht einen Betreuer.
Die Aufgaben des Betreuers richten sich nach der Hilfsbedürftigkeit des Betreuten. In seinem Aufgabenkreis vertritt der Betreuer den Betreuten gerichtlich und außergerichtlich. Als gesetzlicher Vertreter kann der Betreuer somit auch das Akteneinsichtsrecht des Betreuten wahrnehmen.

Zu Unrecht, denn Betreuer haben in solchen Fällen ein **Auskunfts- bzw. Akteneinsichtsrecht** nach § 18 Landesdatenschutzgesetz. Betroffener ist zwar der Betreute, aber das Akteneinsichtsrecht kann in bestimmten Fällen auch von Dritten ausge-

übt werden. So könnte z.B. auch ein Rechtsanwalt zur Wahrnehmung des Akteneinsichtsrechts bevollmächtigt werden. Für das Betreuungsrecht gilt, daß der Betreuer in dem Aufgabenbereich, für den er bestellt wurde, der gesetzliche Vertreter des Betreuten ist. Aus diesem Grund steht ihm auch das Akteneinsichtsrecht zu.

Nachdem die Klinik trotz mehrfacher Aufforderung noch nicht einmal eine Stellungnahme abgegeben hatte, haben wir die **Aufsichtsbehörde** eingeschaltet, die eine **Weisung** in unserem Sinn erteilte. Inzwischen wurde der Entlassungsbericht an den Betreuer übersandt.

Was ist zu tun?
Kliniken müssen Betreuern in derartigen Fällen Akteneinsicht gewähren.

4.8.6 Meldungen der Gesundheitsämter an den Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten

Künftig wird es nur noch anonymisierte Meldungen der Gesundheitsämter geben. Das Sozialministerium reagierte erst zehn Jahre nach unserer Kritik.

Im Rahmen der Überprüfung eines Gesundheitsamtes im Jahre **1986** hatten wir festgestellt, daß die Gesundheitsämter die nach dem Bundesseuchengesetz gemeldeten übertragbaren Krankheiten grundsätzlich an den „Beauftragten für die systematische Bekämpfung des Typhus, Paratyphus B, sonstiger Salmonellosen sowie der Hepatitis und Meningitis" weiter übermitteln. Nach dem Bundesseuchengesetz ist aber weder ein solcher Beauftragter noch eine derartige Übermittlung vorgesehen.

Unserer Kritik schloß sich eine **jahrelange Diskussion** mit dem Ministerium für Arbeit, Gesundheit und Soziales des Landes Schleswig-Holstein an. Es wurden immer neue Überlegungen angestellt, ob man eine ausreichende Rechtsgrundlage schaffen könnte, zuletzt war für die vergangene Legislaturperiode eine solche im Rahmen der beabsichtigten Novellierung des Gesundheitsdienstgesetzes vorgesehen. Da das Fachministerium immer wieder dargelegt hatte, wie wichtig diese Meldungen seien, wurde zunächst übergangsweise im Hinblick auf die angekündigte gesetzliche Regelung die Fortführung der Meldungen an den Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten nicht beanstandet.

Nachdem inzwischen eine neue Legislaturperiode angebrochen ist und nach nunmehr zehn Jahren noch immer kein Entwurf einer Novelle für das Gesundheitsdienstgesetz vorliegt, haben wir das Ministerium erneut gemahnt. Es hat daraufhin mitgeteilt, daß es an einer Umstrukturierung der Aufgaben des Beauftragten für die systematische Bekämpfung über-

tragbarer Krankheiten arbeite. Außerdem wurde angeordnet, daß ab **sofort** die Datensätze von den Gesundheitsämtern lediglich in **anonymisierter Form** geliefert werden.

4.9 Kultusbereich

4.9.1 Verwendung privater PC durch Lehrer

Immer mehr Lehrer arbeiten mit privaten PC. Vom Gesetzgeber wird überlegt, ob ihnen weiterhin verboten bleiben soll, diese zur Verarbeitung von Schülerdaten zu verwenden.

Schülerdaten erhält ein Lehrer nur aus seiner dienstlichen Aufgabenstellung heraus und darf sie nur zu dienstlichen Zwecken verwenden. Sie bleiben **Daten der Schule**. Bei Verarbeitung schulischer Daten auf privaten PC der Lehrkräfte sind Schulen jedoch nicht in der Lage,

- die Speicherung dienstlicher Daten in Dateien zu prüfen,
- für die Löschung entbehrlicher Daten zu sorgen,
- den Zugang zu den Daten zu kontrollieren und
- zu verhindern, daß Daten aus dem Verfügungsbereich der Lehrer hinausgelangen.

Konsequenterweise erklärt das Schulgesetz bislang die Benutzung privater PC durch Lehrer für unzulässig.

Diese Bestimmung ist seither immer wieder Stein des Anstoßes gewesen. Lehrer, die im häuslichen Bereich ihre Arbeit weitgehend mit Hilfe von Datenverarbeitungsgeräten erledigen, verstehen nicht, warum z.B. die Korrektur von Arbeiten der Schüler selbstverständlich zu Hause durchgeführt werden darf, Bemerkungen in Notizbüchern selbstverständlich zu Hause verwahrt werden dürfen und die Erledigung von Dienstpost mit der Typenhebelschreibmaschine zulässig, die Verwendung eines komfortableren, gerade neu angeschafften PC aber verboten ist. Ergänzt wird diese Aufzählung dann üblicherweise noch durch den Hinweis, daß Lehrkräfte entweder als Beamte in einem besonderen Treueverhältnis zum Dienstherrn stünden oder als Angestellte für den öffentlichen Dienst besonders ausgebildet und verpflichtet seien. Man müsse ihnen doch vertrauen. Beschwerden zeigen allerdings immer wieder, daß gegen das Schulgesetz verstoßen wird (vgl. 18. TB, Tz. 4.9.4) und personenbezogene Daten auf dem **häuslichen PC** verarbeitet werden. Gelegentlich wird das auch mehr oder weniger offen zugegeben. Konsequenzen hat das Kultusministerium bislang aber nicht gezogen.

An einer Bestimmung, deren Sinn die Betroffenen nicht einsehen und die sie - offenbar ohne Folgen - in nicht unerheblichem Maß verletzen, kann dem Datenschutz nicht gelegen sein. Eine schlechte Alternative zu dem Verbot der Benutzung „außerschulischer" PC wäre allerdings die totale Freigabe. Auch das würde den Gefahren für das informationelle Selbstbestimmungsrecht der Schüler und Eltern nicht gerecht. Dies um so mehr, als nicht wenige Lehrer inzwischen einen Internetanschluß besitzen, ohne daß ihr PC gegen Angriffe fremder Hacker hinreichend gesichert wäre. Was erreicht werden muß, ist deshalb ein Verfahren im Umgang mit Schuldaten, das die Verwendung moderner technischer Arbeitsmittel gestattet, den Beteiligten die Sensibilität der Informationen und der Verarbeitungstechnik deutlich macht, wirkungsvolle Hilfen für ausreichenden Datenschutz anbietet, Risiken für das informationelle Selbstbestimmungsrecht minimiert und Verstöße gegen Schutzvorschriften auch im Bewußtsein der Lehrkräfte als rechtswidriges Handeln erscheinen läßt.

Die **F.D.P.-Landtagsfraktion** hat die Initiative ergriffen und einen Gesetzentwurf zur Aufhebung des Verbots der Nutzung privater PC eingebracht. Inzwischen liegt auch ein entsprechender Regierungsentwurf vor.

Wenn das bisherige strikte Verbot der Benutzung privater Datenverarbeitungsgeräte nicht mehr gelten soll, erscheint ein **Genehmigungsvorbehalt** für eine Benutzung privater PC zwingend. Vor allem aber kommt es darauf an, daß in einer **ergänzenden Rechtsverordnung** klare Detailregelungen getroffen werden. Hierzu gehören die technischen und organisatorischen Maßnahmen, die gewährleistet sein müssen, wenn die Verarbeitung auf privaten PC genehmigungsfähig sein soll. In diesem Zusammenhang wird es darum auch notwendig sein, zu einem ausgewogenen und schlüssigen Gesamtkonzept der technischen und organisatorischen Maßnahmen zu kommen, das auch die konventionelle häusliche Datenverarbeitung nicht ausklammert. Denn die betroffenen Lehrer würden es nicht verstehen, wenn sie beim Einsatz von PC Datensicherheitsmaßnahmen zu beachten hätten, bei konventioneller Datenverarbeitung aber vermeintlich nicht.

Außerdem sind weitere Regelungen, z.B. zur Löschung personenbezogener Daten, zu treffen. Nachdem wir jahrelang vergeblich auf den Erlaß einer Verordnung nach § 50 Abs. 7 Schulgesetz gedrängt haben, erscheint es uns allerdings unabdingbar, daß die Verordnung **zeitgleich** mit der beabsichtigten **Novellierung** des Schulgesetzes in Kraft tritt, weil ohne sie die gesetzliche Regelung ein Torso bliebe.

Im Wortlaut: § 50 Abs. 7 Schulgesetz
Soweit ... regelt die Ministerin oder der Minister für Bildung, Wissenschaft, Jugend und Kultur durch Verordnung:

1. *den zulässigen Umfang der Verarbeitung von Daten,*
2. *die Datenübermittlung,*
3. *die Sperrung, Löschung und Aufbewahrung von Daten,*
4. *die Datensicherung,*
5. *die automatisierte Datenverarbeitung.*

Was ist zu tun?
Die Novellierung des Schulgesetzes und der Erlaß einer begleitenden Verordnung sollten ohne Zögern in die Tat umgesetzt werden. Das Verbot der Nutzung privater PC darf allerdings nur aufgehoben werden, wenn eine bessere Lösung zur Verfügung steht.

4.9.2 Was die Zusicherung der Vertraulichkeit wert war

Wird Bürgern, die freiwillig öffentlichen Stellen Informationen geben, ausdrücklich Vertraulichkeit zugesichert, unterliegen die erhaltenen Auskünfte einer besonderen Zweckbindung. Ohne Einverständnis der Betroffenen dürfen sie nicht anderweitig verwendet werden.

Eine Amtsverwaltung bat die Eltern, in einer Fragebogenaktion zur Einführung von festen Grundschulzeiten Stellung zu nehmen. In ihrem Anschreiben wies sie auf die **Freiwilligkeit der Befragung** hin und versicherte, daß die gemachten Angaben nur zu statistischen Zwecken ausgewertet und **vertraulich** behandelt würden. Im Fragebogen wurde auch nach Namen und Anschrift gefragt.

Ein Vater beantwortete die gestellten Fragen nicht nur durch Ankreuzen der vorgegebenen Antwortkästchen, sondern begründete auf der Rückseite des Fragebogens den Besuch seines Kindes in einer weiter entfernten Schule damit, daß in der näher gelegenen Schule seines Wohnortes eine Lehrkraft Kinder schlage. Es war nach unserer Auffassung eindeutig, daß der Petent diese Äußerung nicht als Anzeige verstanden wissen wollte, sondern lediglich als erläuternde Sachäußerung. Kaum war der Fragebogen bei der Amtsverwaltung abgegeben, erhielt der Petent eine Vorladung der Polizei, weil ein **Ermittlungsverfahren** wegen Verdachts der Verleumdung bzw. übler Nachrede gegen ihn eingeleitet worden war.

Die Amtsverwaltung hatte nämlich sofort den zuständigen **Schulleiter informiert**. Daraufhin erstatteten alle Lehrkräfte dieser Schule Anzeige gegen den Petenten. Die Angelegenheit eskalierte derart, daß zum Schluß ein Strafprozeß geführt wurde. Dieser endete zwar mit einer Einstellung des Verfahrens, der Petent mußte jedoch seine eigenen Kosten tragen.

Wir haben gegenüber der Amtsverwaltung **beanstandet**, daß die Angaben des Petenten ohne vorherige Rücksprache mit ihm an andere Stellen übermittelt worden sind. Der Hinweis der Verwaltung, die Angaben auf der Rückseite des Fragebogens unterlägen nicht der Vertraulichkeit, weil sie nicht in das vorgegebene Antwortschema paßten, konnten wir nicht gelten lassen.

Dieser Fall zeigt deutlich, wie wichtig die Beachtung der Zweckbindungsvorschriften des Landesdatenschutzgesetzes ist. Das Gesetz schränkt die Verarbeitung von Daten für andere Zwecke ohne Einwilligung des Betroffenen ausdrücklich ein, wenn die gemachten **Angaben freiwillig für einen bestimmten Zweck** zur Verfügung gestellt wurden.

Was ist zu tun?
Die öffentlichen Stellen müssen mit freiwillig zur Verfügung gestellten Informationen sehr sorgfältig umgehen. In Zweifelsfällen sollte zunächst Kontakt mit dem Betroffenen selbst aufgenommen werden.

4.10 Steuerverwaltung

4.10.1 Stört das Steuergeheimnis den „schlanken Staat“?

Aus wirtschaftlichen Überlegungen werden die Großrechenzentren der Steuerverwaltung und der Datenzentrale zusammengelegt. Fast wäre dabei das Steuergeheimnis auf der Strecke geblieben.

Seit 1967 bedient sich die schleswig-holsteinische Steuerverwaltung für die Festsetzung und Erhebung der Steuern automatisierter Verfahren. Jährlich werden mit Hilfe von Computern **mehrere Millionen Steuererklärungen** versandt, Buchungen vorgenommen sowie **Steuerbescheide**, Zahlungsaufforderungen, Mahnungen und dgl. gedruckt. Gegen stattliche Leistungsentgelte hat die Datenzentrale deshalb im Gebäude der Oberfinanzdirektion ein Großrechenzentrum installiert, das von einer kleinen Crew von DZ-Mitarbeitern technisch betreut wird. Ansonsten schaltet und waltet die Oberfinanzdirektion entsprechend den von ihr festgelegten Prioritäten. Mit den technischen Systemen werden ausschließlich Steuerdaten verarbeitet, die elektronische Kommunikation zwischen den Finanzämtern und dem Rechenzentrum wird von der Oberfinanzdirektion gesteuert, sie selbst entwickelt, testet und bestimmt den Einsatz der Programme usw. Im Ergebnis bekommt also kein Mitarbeiter der DZ Kenntnis vom Inhalt der Millionen Steuerdaten und der Ergebnisse der

maschinellen Bearbeitungen. Dies alles wurde 1975 in einem detaillierten Vertrag so geregelt, um den Bestimmungen des Finanzverwaltungsgesetzes zu entsprechen und das **Steuergeheimnis** zu wahren. Eine von uns im Jahre 1986 durchgeführte Prüfung gab deshalb insoweit auch keinen Anlaß zu datenschutzrechtlichen Beanstandungen.

Der parallele Betrieb von zwei Rechenzentren, eines im Gebäude der Oberfinanzdirektion und eines in der Zentrale in Altenholz, lief offenbar in den letzten 20 Jahren zur allseitigen Zufriedenheit, bis Anfang 1996 vom Innenministerium als dem Verwalter des Landesanteils der DZ und vom Finanzministerium als dem Zahler der Leistungsentgelte die Prüfung veranlaßt wurde, ob nicht durch ein Zusammenlegen der Rechenzentren ein Synergieeffekt erzielt werden könnte. Im Rahmen des **„Projektes zur Integration der Rechenzentren von Landes- und Steuerverwaltung (PILS)"** haben sich die Beteiligten recht schnell darüber verständigt, daß die finanzverfassungsrechtlichen Bestimmungen des Finanzverwaltungsgesetzes nicht grundsätzlich einer Zusammenlegung entgegenstünden und das Steuergeheimnis nicht tangiert sei. Es schien also möglich, das Rechenzentrum in der Oberfinanzdirektion aufzulösen und die betreffenden Arbeiten von Mitarbeitern der Datenzentrale in Altenholz miterledigen zu lassen.

Stichwort: Steuergeheimnis
Das Steuergeheimnis ist ein „qualifiziertes Amtsgeheimnis", das restriktiver ist als die allgemeine Amtsverschwiegenheit. Die Pflicht, das Steuergeheimnis zu wahren, ist das Gegenstück zu den weitreichenden Mitwirkungspflichten (Abgabe von Steuererklärungen) der Steuerpflichtigen. Die zulässigen Durchbrechungen des Steuergeheimnisses sind in § 30 Abgabenordnung abschliessend aufgeführt.

Um so erstaunter war man, als wir wegen einer möglichen Gefährdung des **Steuergeheimnisses** Bedenken anmeldeten. Maßgeblich waren folgende Gesichtspunkte:

- Das Projekt war nicht in Gang gesetzt worden, um auch in Zukunft eine ordnungsgemäße Abwicklung der Besteuerungsverfahren durch die Finanzbehörden zu gewährleisten, sondern um „im Sinne der Verbesserung der Gesamtwirtschaftlichkeit **Kosten zu reduzieren**" und „durch die Integration der Rechenzentren mittelfristig zu einer deutlichen **Haushaltsentlastung** zu gelangen" (so die Formulierungen in den „Projektzielen").

- Die einschlägigen finanzverfassungsrechtlichen und steuerverfahrensrechtlichen Fragestellungen waren bereits im Jahr 1975 einer eingehenden Prüfung unterzogen worden. Man ist damals zu einer **anderen rechtlichen Beurteilung** gekommen.

- Die „bereichsspezifische" Rechtslage hat sich zwischenzeitlich nicht geändert. Vielmehr hat die Verfassungsgerichtsrechtsprechung zum informationellen Selbstbestimmungsrecht die **Bedeutung der besonderen Berufs- und Amtsgeheimnisse** eher noch betont.

Die rechtlichen „Grenzwerte" sind also seitens der **Steuerverwaltung** 1975 richtigerweise in der Formulierung zusammengefaßt worden, daß „die Steuerverwaltung verantwortlich sämtliche Maßnahmen des Datenschutzes und der Datensicherheit **entscheidet** und dadurch das Steuergeheimnis gewährleistet". Ein Abweichen von diesem Grundsatz im Rahmen des Projektes PILS wäre mithin gleichzusetzen gewesen mit einer Änderung der Rechtsauffassung zu den Wirkungen des Finanzverwaltungsgesetzes und der Abgabenordnung.

Nachdem man diesen Gesichtspunkten in der Anfangsphase der Arbeit der Projektgruppe eher **ablehnend** gegenüberstand, konnten wir im weiteren Verlauf eine weitgehende **Annäherung der Standpunkte** erreichen. Dadurch, daß in einer besonderen Organisationseinheit in der Datenzentrale Mitarbeiter der Steuerverwaltung die Verarbeitungsprozesse steuern und überwachen, hat man nämlich eine aufbau- und ablauforganisatorische Grundstruktur geschaffen, die geeignet ist, dem allgemeinen datenschutzrechtlichen und dem bereichsspezifischen steuerrechtlichen Rahmen Rechnung zu tragen. Das gilt allerdings nur unter **zwei Bedingungen**:

- Die noch zu formulierenden Service-Vereinbarungen müssen im Ergebnis sicherstellen, daß die Mitarbeiter der DZ die Inhalte steuerlicher Datenbestände und umgekehrt die Mitarbeiter der Oberfinanzdirektion die Inhalte sonstiger Datenbestände (z. B. polizeiliche Daten, Personaldaten) nicht zur Kenntnis nehmen können.

- Die personelle Besetzung der geplanten besonderen Organisationseinheit muß auf Dauer so gestaltet sein, daß den Soll-Regelungen in den Vereinbarungen auch das tatsächlich erforderliche „Ist" gegenübersteht.

Was ist zu tun?

Die öffentlichen Stellen müssen bei ihren Verschlankungsbemühungen in Rechnung stellen, daß es sich bei den besonderen Berufs- und Amtsgeheimnissen, zu denen neben dem Arzt-, Sozial-, Statistik-, Post- und Fernmeldegeheimnis auch das Steuergeheimnis gehört, um so fundamentale Rechtsgüter handelt, daß wirtschaftliche Interessen allein eine Aufweichung nicht rechtfertigen können.

4.10.2 Auf den ersten Blick ein klarer Fall ...

Es ist den Betroffenen kaum zu vermitteln, daß sich die höchstrichterliche Rechtsprechung manchmal über den klaren Wortlaut gesetzlicher Bestimmungen hinwegsetzt.

Manche Beschwerden von Bürgern weisen so eindeutig auf fehlerhaftes Verwaltungshandeln hin, daß man geneigt ist, gar nicht erst eine Stellungnahme der kritisierten Behörde einzuholen, sondern gleich eine datenschutzrechtliche Beanstandung auszusprechen. So auch in folgendem Fall: Ein Unternehmer bekam an seine Firmenanschrift einen Brief eines Finanzamtes mit **Postzustellungsurkunde** zugestellt. Außen auf dem Briefumschlag war vermerkt: „Geschäftszeichen 2021013972 Pfändung vom 14.05.1996“ (Anmerkung: Die Daten sind geändert). Der Empfänger empfand es als einen Bruch des Steuergeheimnisses, den **Briefinhalt außen auf dem Umschlag** zu vermerken, zumal nicht er der Steuerschuldner war, sondern einer seiner Lieferanten. Es war lediglich dessen Forderung gegen ihn gepfändet worden, deshalb war er als **Drittschuldner** verpflichtet, nicht an den Lieferanten zu zahlen, sondern an das Finanzamt. Nur, jeder der den Umschlag in den Händen hielt, mußte vermuten, dem Unternehmen ginge es so schlecht, daß wegen Steuerschulden gepfändet werden müßte.

Das Verwaltungszustellungsgesetz gab dem Petenten (vermeintlich) recht. Dort ist festgelegt: „Die Sendung ist mit der Anschrift des Empfängers und mit der Bezeichnung der absendenden Dienststelle, einer **Geschäftsnummer** und einem Vordruck für die Zustellungsurkunde zu versehen“. Folglich war nur die Steuernummer korrekt, alles weitere unzulässigerweise vermerkt, möchte man glauben. In ihren Stellungnahmen kamen das Finanzamt und die Oberfinanzdirektion unter Hinweis auf die Rechtsprechung des **Bundesfinanzhofes** (BFH) allerdings zu einem ganz anderen Ergebnis. Zitat aus einem Urteil des BFH aus dem Jahre 1990: „Daher liegt nach ständiger Rechtsprechung des BFH eine zwingende Verletzung des § 3 Abs. 1 Satz 2 Verwaltungszustellungsgesetz vor, wenn die zuzustellende Sendung (d.h. der verschlossene Umschlag) nicht mit einer ausreichenden, den Inhalt der Sendung einwandfrei identifizierenden Geschäftsnummer versehen ist. ... Dabei stellt die Angabe der Geschäftsnummer auf der Sendung und in der Postzustellungsurkunde die einzige urkundliche Beziehung zwischen dieser und dem zuzustellenden Schriftstück her. Es genügt somit für eine wirksame Zustellung nicht, wenn die Postzustellungsurkunde und/oder die Sendung (der Briefumschlag) als Geschäftsnummer lediglich die Steuernummer ausweist.“ Da unter einer Steuernummer sehr unterschiedliche Unterlagen zugestellt werden könnten, sei eine **ergänzende Angabe** des Inhalts **zwingend erforderlich** gewesen. Allerdings hätte das Finanzamt das Wort „Pfändung“ durch eine geeignete Abkürzung ersetzen müssen. Offen blieb die Frage, welche Abkürzung einerseits „geeignet“ gewesen

wäre, den Inhalt zu beschreiben, andererseits Dritten nicht offenbart hätte, daß es sich um einen Pfändungsvorgang handelte.

Uns blieb nur die Aufgabe, den Betroffenen mit dem Hinweis zu „trösten", daß auch ein Datenschutzbeauftragter die Rechtsprechung des höchsten deutschen Finanzgerichts nicht vom Tisch wischen kann, er aber andererseits Verständnis für sein Unverständnis über das Ergebnis aufbringe.

Was ist zu tun?
Das Finanzministerium sollte die Finanzämter anweisen, die zusätzlichen Vermerke so zu gestalten, daß sie nicht fehlinterpretiert werden können bzw. das Steuergeheimnis verletzen, in diesem Fall z.B. durch den Begriff „Inanspruchnahme als Drittschuldner".

4.10.3 Eine Sache der Logik

Die Finanzämter fordern in bestimmten Fällen von Apothekern personenbezogene Angaben über ihre Kunden, ohne daß sie mit den Daten etwas anfangen können. Eine sinnvolle Ausnahmeregelung von einer bundeseinheitlichen Richtlinie über Fahrtenbücher wurde vom Ministerium abgelehnt.

Benutzt ein Unternehmer einen Pkw für Geschäftsreisen, kann er die entstehenden Kosten als Betriebsausgaben geltend machen. Benutzt er ihn für private Zwecke, sind die Kosten steuerlich nicht abzugsfähig. Um die jeweiligen Kostenanteile einfach ermitteln zu können, wenn ein Pkw sowohl geschäftlich wie auch privat genutzt wird, sieht das Einkommensteuergesetz eine Pauschalierung vor. Wer sich dieser nicht unterwerfen will, muß ein **Fahrtenbuch** führen, damit jeder Kilometer „spitz" abgerechnet werden kann. In den Fällen hoher geschäftlicher und niedriger privater Anteile stellt eine Abrechnung nach Fahrtenbuch die steuergünstigere Alternative dar. Man muß allerdings in Kauf nehmen, daß die Finanzämter im Fahrtenbuch folgende Angaben erwarten: Datum, Kilometerstand zu Beginn und am Ende der einzelnen Fahrt, Reiseziel mit Reiseroute, Reisezweck mit **Angabe des aufgesuchten Geschäftspartners**, jeweilige Abfahrt- und Ankunftzeit; Privatfahrten müssen einzeln, jedoch ohne Angabe des Reiseweges aufgezeichnet werden.

Gegen die Angabe des „aufgesuchten Geschäftspartners" in dem Fahrtenbuch für einen Pkw, mit dem Mitarbeiter einer Apotheke eilige Arzneimittel an behinderte oder bettlägerige Kranke ausliefern, wandte sich ein Apotheker. Die Angabe des Geschäftspartners/Kunden könne nur dazu dienen, anhand der sonstigen Buchführungsunterlagen die Frage zu klären, ob die aufgesuchte Person tatsächlich ein Geschäftspartner/Kunde sei. Finde sich der Name in Verträgen oder Rechnungen wieder, läge es

nahe, daß ein Besuch bei ihm geschäftlich veranlaßt gewesen sei, anderenfalls bedürfte es weiterer Begründungen, um einen Betriebsprüfer des Finanzamtes von der Anerkennung der Fahrtkosten als Betriebsausgabe zu überzeugen. Man könne ihn deshalb nicht dazu zwingen, auch dann ein **Kundenverzeichnis** aufzubauen, wenn viele Kunden entweder bar bezahlten oder die Zahlungen über eine Verrechnungsstelle in einer Summe erfolgten. Dann sei es nämlich völlig egal, ob im Fahrtenbuch „Müller" oder „Meier" stehe, es biete dem Betriebsprüfer ohnehin keine Kontrollmöglichkeit, weil es keinen „Gegenbeleg" gebe. Da sei es nur eine Frage der Logik, ganz auf eine Namensnennung und damit auf einen **nutzlosen**, gleichwohl **hochsensiblen** Datenbestand zu verzichten.

Dieser Argumentation konnten wir uns ungeschränkt anschließen und waren deshalb überrascht, daß das **Ministerium für Finanzen und Energie** dieses Ansinnen **ablehnte**, ohne auf den Kern der Sache, nämlich die Auswertungsmöglichkeiten, einzugehen. Vollends unverständlich wird die Entscheidung, wenn man berücksichtigt, daß Ärzte, die regelmäßig Hausbesuche machen (sogenannte Vielfahrer) im Fahrtenbuch nur „Patientenbesuch" vermerken müssen. Nicht daß der Datenschutzbeauftragte gegen diese Ausnahmeregelung votieren will, im Gegenteil. Wer erklärt aber dem Apotheker, daß ein Arzt, bei dem ein Abgleich mit der Patientendatei durchaus möglich wäre, von der Angabe des Namens der besuchten Person befreit ist, während er einen nicht verwertbaren personenbezogenen Datenbestand führen muß. Wahrscheinlich wird er nur stöhnen: „Heiliger St. Bürokratius, halt ein!".

Was ist zu tun?
Das Ministerium für Finanzen und Energie sollte „Größe zeigen" und den Regeln der Logik Geltung verschaffen. Dazu bedarf es nicht einmal einer Gesetzesänderung, sondern nur der Einfügung von zwei Worten („und Apotheker") in einer Verwaltungsanweisung.

4.11 Personalwesen

4.11.1 Beihilfedaten nicht abgeschottet

Eine Amtsverwaltung bediente sich zur Beihilfeberechnung einer privaten Versicherung. Das Verfahren verstieß gegen Vorschriften des Beamten- und des Datenschutzgesetzes.

Früher waren die Beihilfefälle eines Amtes über den Kreis abgewickelt worden. Als dieser der Beihilfekasse der Versorgungsausgleichskasse der Kommunalverbände (VAK) beitrat, endete dieses Verfahren. Das Amt ließ nunmehr die **Beihilfeberechnung durch eine private Versicherung** durchführen und erteilte auf dieser Grundlage den Beihilfebescheid. Der Petent war mit der Weitergabe seiner Daten an die Versicherung nicht einverstanden, verweigerte die erbetene Einwilligung dazu und bat um

datenschutzrechtliche Überprüfung der Beihilfeorganisation. Wir mußten verschiedene datenschutzrechtliche Verstöße beanstanden.

Zulässig wäre das Verfahren dann gewesen, wenn das Amt in vollem Umfang datenverarbeitende Stelle geblieben wäre und die Versicherung nur im Rahmen der Auftragsdatenverarbeitung eingeschaltet hätte. Dieser Rahmen war im vorliegenden Fall jedoch überschritten. Denn die Versicherung nahm nicht nur Hilfsfunktionen - wie im Auftragsverhältnis üblich - wahr, sondern hatte in Wirklichkeit eigene Wertungen und Entscheidungen zu treffen. Folglich würden ihr die Daten nicht als Auftragnehmerin überlassen, sondern wie an einen Dritten übermittelt.

Da jedenfalls für die Beamten eine Norm als Rechtsgrundlage für diese Datenübermittlung fehlte, konnte das Verfahren **nur mit Einwilligung der Betroffenen** rechtmäßig durchgeführt werden. Der Petent hatte die Einwilligung versagt. Daraufhin teilte ihm das Amt mit, sein Antrag könne daher „zur Zeit nicht bearbeitet werden".Aufgrund unserer Prüfung mußte die Amtsverwaltung seinen Beihilfeanspruch selbst berechnen.

Andere Beamte hatten ihre Einwilligung gegeben. Wir stellten aber fest, daß sie **nicht** in der vom Landesdatenschutzgesetz geforderten Weise über die Bedeutung der Einwilligung **aufgeklärt** worden waren. So wurden z.B. die Betroffenen nicht darüber aufgeklärt, daß die Verweigerung der Einwilligung mit keinerlei Rechtsfolgen für sie verbunden war. Deswegen haben wir eine Beanstandung ausgesprochen.

Schließlich war zu kritisieren, daß die vom Landesbeamtengesetz geforderte **Trennung der Beihilfeakten von den übrigen Personalakten** hier deshalb nicht eingehalten war, weil derselbe Bearbeiter in der Amtsverwaltung sowohl die Personalangelegenheiten als auch die Beihilfen zu bearbeiten hatte. Das Landesbeamtengesetz fordert diese Trennung jedoch, um zu vermeiden, daß Erkenntnisse über den Gesundheitszustand der Betroffenen und seiner Familie, wie sie aus der Beihilfebearbeitung zwangsläufig erwachsen, unmittelbar Eingang in personalrechtliche Entscheidungen finden können. Die Organisation des Beihilfeverfahrens mußte auf unsere Beanstandung hin umgestellt werden.

Wenn in kleinen Kommunen die Trennung der Bereiche Beihilfe und Personalverwaltung nicht möglich ist, bietet sich die Einschaltung der Versorgungsausgleichskasse der Kommunalverbände als Lösung an.

Was ist zu tun?
Die Behörden sollten überprüfen, ob bei ihnen die Abschottung der Beihilfe- von der Personalsachbearbeitung gewährleistet ist.

4.11.2 Muß der Betroffene seiner Personalakte hinterherfahren?

Der Beamte hat nicht nur ein Recht auf Einsicht in seine Personalakte; es muß ihm auch Gelegenheit dazu unter zumutbaren Bedingungen gegeben werden. Ein Petent mußte zwei Jahre auf die Gewährung von Akteneinsicht warten.

Ein langer Weg lag vor ihm, als ein Lehrer im Juni 1994 schriftlich beim Bildungsministerium **Einsicht in seine Personalakte** erbat. Der Brief kam nach zwei Wochen mit dem lapidaren Zusatz „Dienstweg!“ zurück, denn der Beamte hatte den kürzeren, unmittelbaren Postweg gewählt. Anfang Juli 1994 schrieb er nunmehr auf dem Dienstweg noch einmal - und wartete fast ein Jahr vergeblich auf Antwort. Der Brief war verlorengegangen, wie sich später herausstellte. Im Juni 1995 versuchte er zum dritten Mal, Kontakt zu seinem Dienstherren aufzunehmen. Schon ein Vierteljahr später hatte er die Antwort (ebenfalls auf dem Dienstweg) in den Händen, aber viel konnte er damit nicht anfangen. Denn man bestätigte ihm - er wußte es schon vorher - , daß er wie jeder Landesbedienstete das Recht auf Einsicht in seine Personalakte habe. Die Personalakte dürfe aber nicht an seine Schule übersandt werden, er müsse sich schon nach Kiel auf den Weg machen, um während der Dienstzeit in einem bestimmten Dienstzimmer des Ministeriums in die Akte Einsicht zu nehmen.

Das hätte, so schrieb uns der Petent, Unterrichtsausfall für einen Schultag bedeutet, den er wegen einer Stunde Akteneinsicht seinen Schülern nicht zumuten wollte. Er wandte sich statt dessen an uns. Zwei Erinnerungen waren notwendig, bis uns aus dem **Bildungsministerium** die Nachricht erreichte, man arbeite an einer allgemeinen Regelung. Diese solle nach Wahl der Lehrkraft Akteneinsicht in der Schule bzw. bei den Schulämtern oder im Ministerium möglich machen. Im Juni 1996 - also zwei Jahre nach seinem ersten Versuch - hat der Lehrer schließlich Aktensicht erhalten - ein Vorgang, der ihn dann weniger als eine Stunde kostete. Bleibt festzustellen, daß im konkreten Fall endlich doch gut wurde, was lange währte. Nur - muß für richtige Entscheidungen eines Ministeriums wirklich erst eine „allgemeine Regelung“ in die Welt gesetzt werden?

Was ist zu tun?
Gewährt der Gesetzgeber Betroffenen Rechte, so muß die Verwaltung, ihnen die Ausübung dieser Rechte auch unter zumutbaren Bedingungen ermöglichen.

4.11.3 Moderne Verwaltung und die Personalakten

Im Rahmen von Verwaltungsreformen werden auch Modelle der dezentralen Personalverwaltung diskutiert. Sie sind dann zulässig, wenn die Schutzvorschriften des Personalaktenrechts beachtet werden.

Im Rahmen von **Modernisierungsüberlegungen** einer Stadtverwaltung sollten auch Personalverwaltungsangelegenheiten auf die einzelnen Ämter verlagert werden. Zu diesem Zweck waren in sogenannten Pilotkontrakten Tabellen erstellt worden, die die einzelnen zu dezentralisierenden Personalverwaltungsvorgänge auflisteten und die Beteiligungsrechte der unterschiedlichen Stellen an den Entscheidungen darstellten. Hierüber und über die exakte Abgrenzung der zulässigen Verarbeitung von Personalaktendaten zwischen dem zentralen Personalamt und den dezentralen Stellen bestanden innerhalb der Stadtverwaltung Meinungsverschiedenheiten und Unsicherheiten. Denn nach § 106 a Abs. 3 Landesbeamtengesetz (LBG), das insoweit nach dem Landesdatenschutzgesetz auch für Angestellte und Arbeiter gilt, dürfen **Zugang zur Personalakte** nur wenige Beschäftigte haben.

> ***Im Wortlaut: § 106 a Abs. 3 LBG***
> *Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und nur, soweit dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren. Zugang zur Personalakte hat ebenfalls die oder der Geheimschutzbeauftragte im Rahmen von Sicherheitsüberprüfungen.*

Mußten nun deshalb die Personalverwaltung weiterhin zentral geführt und die dezentralen Stellen im Bedarfsfall nur mit einzelnen Informationen „versorgt" werden? Oder mußte in jeder dezentralen Einheit eine eigene Personalverwaltungsorganisation die bisherigen Aufgaben anstelle des zentralen Personalamts übernehmen? Oder war eine „mittlere" Lösung möglich, die die Nutzung von Personalakten durch Mitarbeiter der dezentralen Einheiten zuließ und ihnen einen eigenen dezentralen Entscheidungsspielraum eröffnete?

Die Stadt bat um unsere Beratung.

Aufgrund der **besonderen Vertraulichkeit der Personalakten**, die im Landesbeamtengesetz garantiert ist, kommt es darauf an,

- den Zugriff auf Personalaktendaten einzuschränken und dadurch
- den Kreis der Wissensträger über vollständige Personalvorgänge möglichst klein zu halten sowie

- Interessenkollisionen zu verhindern, die dadurch entstehen können, daß Wissensträger Informationen aus den Personalakten auch in anderen Verwaltungszusammenhängen verwenden.

Aus diesen Beschränkungen folgt, daß die **Personalaktenführung** immer bei einer **Personalverwaltungsstelle** liegen muß. Dabei liegt es in der Organisationsentscheidung der Behörde, wie die Personalverwaltungsstelle organisiert und wo sie angesiedelt ist. Sie kann zentral für mehrere Dienststellen zuständig sein. Eine dezentrale Wahrnehmung der Aufgaben ist jedoch ebenfalls zulässig, insbesondere bei kleinen Verwaltungseinheiten kommt sogar auch eine Übertragung von Personalverwaltungsaufgaben auf solche Mitarbeiter in Betracht, die daneben andere Fachaufgaben zu erfüllen haben. Unzulässig ist allerdings eine auf mehrere Organisationseinheiten verteilte oder gar eine doppelte Personalaktenführung (abgesehen von der Führung von Teilakten und Nebenakten unter den im LBG vorgesehenen Voraussetzungen).

Neben diesen Vorgaben für die Personalaktenführung und den speziellen Zugangsbeschränkungen bestehen für die **Bearbeitung von Personalverwaltungsvorgängen** keine besonderen datenschutzrechtlichen Einschränkungen. Insbesondere können Personalentscheidungen an verschiedenen Stellen vorbereitet und getroffen werden (z. B. dezentrale Ausschreibung von Stellen, Auswahl von Bewerbern, Auswahl zu befördernder Mitarbeiter). Die für diese Entscheidungen erforderlichen Informationen müssen jedoch, soweit sie in die Personalakte gehören, von der Personalverwaltungsstelle im Einzelfall zur Verfügung gestellt und nach entsprechender Verwendung zurückgegeben bzw. gelöscht werden.

Das neue Personalaktenrecht des LBG verhindert also nicht die Delegation oder Dezentralisation von Personalentscheidungen, es schreibt lediglich eine besondere Organisation der Personalakten vor, um einen unkontrollierbaren Zugang zu deren sensiblem Inhalt zu verhindern.

Was ist zu tun?
Behörden, die ihre Struktur „modernisieren", müssen nach Wegen suchen, die den Schutz der Personaldaten ihrer Mitarbeiter sicherstellen.

4.11.4 Bewerbungsunterlagen im Dutzend

Die Verteilung von Bewerbungsunterlagen an alle Mitglieder eines Wahlgremiums ist zwar datenschutzrechtlich zulässig. Es sind aber besondere Maßnahmen zur Datensicherheit zu treffen.

Einige dutzendmal sollten **Bewerbungsunterlagen kopiert** und an alle Mitglieder eines Gremiums verteilt werden, das die Personalentscheidung zu treffen hatte. Ein Bewerber hatte Bedenken gegen die Vervielfältigung der Unterlagen und fragte nach der datenschutzrechtlichen Zulässigkeit solch umfänglicher Verbreitung sensibler personenbezogener Daten. Denn die Bewerbungsunterlagen enthielten wie üblich neben einer Darstellung des beruflichen Werdeganges und sehr persönlichen Angaben unter anderem auch eine Vielzahl von Zeugnissen und ausführlichen Beurteilungen.

Wir vermochten in diesem Vorgang **keine unzulässige Datenverarbeitung** zu erkennen. Alle Mitglieder hatten Anspruch auf den gleichen Informationsstand, weil sie sonst keine Wahlentscheidung hätten treffen können.

Eine andere Frage ist es dagegen, ob die Übersendung von Fotokopien der Bewerbungsunterlagen an alle Mitglieder des Gremiums unter dem Gesichtspunkt der **Datensicherheit** vertretbar ist. Die Übersendung der Bewerbungsunterlagen an viele Personen, die diese Unterlagen in der Regel in ihrem privaten Bereich aufbewahren, stellt objektiv ein Risiko dar. Den Empfängern ist daher in jedem Fall eine Rückgabepflicht aufzuerlegen. Nur bei zwingenden organisatorischen Notwendigkeiten kann eine Mitnahme in den häuslichen Bereich gestattet werden, wobei aber auf eine Verwahrung in geschlossenen Behältnissen gedrungen werden muß.

Was ist zu tun?
Ist eine Vielzahl von Funktionsträgern an einer Personalentscheidung beteiligt, muß die Datensicherheit durch besondere Vorkehrungen gewährleistet werden.

5. Datenschutz bei den Gerichten

5.1 Wenn es im Arbeitsgerichtsprozeß zur Sache geht

Selbst an einem Rechtsstreit gar nicht beteiligte Personen müssen gelegentlich in Kauf nehmen, daß Informationen über sie im Prozeß verwendet werden. In solchen Fällen besteht allerdings die Möglichkeit, die Öffentlichkeit von der mündlichen Verhandlung auszuschließen.

Eine Petentin wandte sich an uns, weil ihr Arbeitgeber plante, wegen wirtschaftlicher Schwierigkeiten seines Betriebes eine Arbeitnehmerin zu entlassen. Nach den Vorschriften des Kündigungsschutzgesetzes hatte er dabei eine sogenannte „soziale Auswahl" zu treffen. Durch diese soll festgestellt werden, welche Arbeitnehmer aus sozialen Gründen am stärksten auf den Arbeitsplatz angewiesen sind und bei welchen eine Kündigung eher zumutbar erscheint. Nachdem die Auswahl des Arbeitgebers anhand dieser Kriterien auf eine bestimmte Beschäftigte gefallen und ihr gekündigt worden war, erhob diese **Kündigungsschutzklage**. Vor dem Arbeitsgericht mußte der Arbeitgeber nun darlegen, warum er gerade dieser Arbeitnehmerin, nicht aber den anderen und auch nicht der Petentin gekündigt hatte. Dazu führte er die Gründe aus, die die Nichtgekündigten aus seiner Sicht besonders schutzwürdig erscheinen ließen. Zu diesem Zweck legte er gegenüber dem Arbeitsgericht schriftlich verschiedene Details über seine Arbeitnehmerinnen dar. Über die Petentin fanden sich in dem Schriftsatz Details über ihre wirtschaftlich problematische Lage, die sie als beschämend empfand. Zu allem Überfluß wurde sie in dem Schriftsatz auch noch als Zeugin für diese Tatsachen benannt, sie mußte daher in dem Kündigungsschutzverfahren, das grundsätzlich öffentlich stattfindet, auftreten. Dabei hätte die Gefahr bestanden, daß die wirtschaftliche Situation der Petentin in der gesamten Belegschaft bekannt würde.

Im Wortlaut: § 171 b GVG

(1) Die Öffentlichkeit kann ausgeschlossen werden, soweit Umstände aus dem persönlichen Lebensbereich eines Prozeßbeteiligten, Zeugen oder durch eine rechtswidrige Tat (§ 11 Abs. 1 Nr. 5 des Strafgesetzbuches) Verletzten zur Sprache kommen, deren öffentliche Erörterung schutzwürdige Interessen verletzen würde, soweit nicht das Interesse an der öffentlichen Erörterung dieser Umstände überwiegt. Dies gilt nicht, soweit die Personen, deren Lebensbereiche betroffen sind, in der Hauptverhandlung dem Ausschluß der Öffentlichkeit widersprechen.

(2) Die Öffentlichkeit ist auszuschließen, wenn die Voraussetzungen des Absatzes 1 Satz 1 vorliegen und der Ausschluß von der Person, deren Lebensbereich betroffen ist, beantragt wird.

(3) Die Entscheidungen nach den Absätzen 1 und 2 sind unanfechtbar.

Aus unserer Sicht konnte die Informationsweitergabe durch den Arbeitgeber nicht beanstandet werden. Die Vorschriften des Kündigungsschutzgesetzes verpflichten ihn, entsprechende Angaben in das Gerichtsverfahren einzuführen. Auch ist es ihm unbenommen, seine Arbeitnehmer als Zeugen in dem Verfahren zu benennen. Allerdings besteht für das Gericht die Möglichkeit, bei der Vernehmung von Zeugen über derartige private Angelegenheiten nach dem Gerichtsverfassungsgesetz (GVG) die **Öffentlichkeit auszuschließen.**

Die Gerichte unterliegen, soweit sie im Rahmen der Rechtsprechung tätig werden, wegen der verfassungsrechtlich garantierten richterlichen Unabhängigkeit keiner Kontrolle. Daher konnten wir den Richter nur im Namen der Petentin dezent auf das Problem aufmerksam machen.

Was ist zu tun?
Die Gerichte sollten von der Möglichkeit des Ausschlusses der Öffentlichkeit von der Verhandlung Gebrauch machen, sobald sich abzeichnet, daß besonders sensible personenbezogene Informationen zur Sprache kommen.

5.2 Strafurteil als Makel fürs Leben?

Trotz der Tilgungsbestimmungen im Bundeszentralregistergesetz werden alte Urteile immer wieder zum Nachteil der Betroffenen verwandt.

Ein wesentlicher Aspekt unseres Strafrechtssystems ist der **Resozialisierungsgedanke**. Nach der Strafvollstreckung soll der frühere Straftäter wieder in die Gesellschaft eingegliedert werden. Damit ihm eine länger zurückliegende Verurteilung nicht auf ewig anhängt, sehen die Vorschriften des Bundeszentralregistergesetzes vor, daß er sich nach Ablauf einer bestimmten Zeit - abhängig von der Höhe der Strafe - als unbestraft bezeichnen darf. Die Straftat und die Verurteilung dürfen dem Betroffenen dann „im Rechtsverkehr" nicht mehr vorgehalten oder zu seinem Nachteil verwertet werden.

Leider kommt es immer wieder zu Verstößen gegen diese Vorschriften. Dies mußte ein Petent erleben, in dessen Wohnung eingebrochen worden war und der nun gegen seine Hausratsversicherung auf Auszahlung der Versicherungssumme klagte. Nachdem er in der ersten Instanz gewonnen hatte, sah er sich in der zweiten Instanz vor dem OLG Schleswig plötzlich mit der **Kopie** eines über zehn Jahre **alten Strafurteils** konfrontiert, das der Rechtsanwalt der Versicherung in das Verfahren eingeführt hatte. Mit dem Hinweis auf die frühere Verurteilung wollte er bei dem Gericht offensichtlich den Eindruck hervorrufen, einer Person, die bereits strafrechtlich aufgefallen war, könne die Schilderung eines Einbruchs nicht

geglaubt werden, und es müsse ein Versicherungsbetrug vorliegen.

Es ist nicht unsere Aufgabe, die Qualität einer solchen Argumentation in einem Zivilprozeß zu bewerten. Allerdings wurden die Vorschriften des Bundeszentralregistergesetzes verletzt. Da die Vorstrafe im Bundeszentralregister inzwischen getilgt war, durfte sie dem Petenten nämlich nicht mehr vorgehalten werden. Leider bleiben die Strafurteile auch nach der Tilgung im Bundeszentralregister in Papierform im Gewahrsam staatlicher Stellen. Nach den Aufbewahrungsbestimmungen für die Justiz lagern sie im Regelfall dreißig Jahre bei der Staatsanwaltschaft. Die Datenschutzbeauftragten haben immer wieder darauf hingewiesen, daß aus dieser zu langen Aufbewahrungsdauer Gefährdungen erwachsen. Für den Rechtsanwalt war es offensichtlich kein Problem, sich das über zehn Jahre alte Strafurteil in Kopie zu besorgen. Bisher konnte trotz Einschaltung der für die datenschutzrechtliche Kontrolle des Anwalts zuständigen Abteilung im Innenministerium noch nicht geklärt werden, auf welchem Wege das Urteil zu dem Anwalt gelangte.

Was ist zu tun?
Strafurteile sollten aus den Unterlagen entfernt werden, wenn die Tilgungsfrist abgelaufen ist.

6. Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung

6.1 Das Pferd von hinten aufgezäumt

Weil die Beschaffung von Informationstechnik zu früh im Mittelpunkt aller Überlegungen steht, bemerken viele Behörden zu spät, daß Planungsfehler sie um die Früchte ihrer Arbeit bringen und ihnen vermeidbare Rechts- und Sicherheitsprobleme bescheren.

Fragt man die für die Informationstechnik (IT) in einer Behörde zuständigen Mitarbeiter nach den **technischen Spezifikationen** der von ihnen betreuten Systeme, sprudeln in der Regel die technischen Details nur so heraus. Da geht es um File-, Datenbank-, Mail-, Fax- und Printserver, um 166 Megahertz getaktete Clients, um Backbone-Netze, Lichtwellenleiter, Controller, Multiplexer, Hubs, X.25, ISDN, X.400, X.500, Gigabyte-Platten, Quad-Speed-CD-ROM-Laufwerke usw. usw. Fragt man nach der **Zielrichtung des IT-Einsatzes**, werden die Antworten etwas weniger wortreich. Da wird von Informations- und Managementsystemen gesprochen, von Bürokommunikation, von struktureller Modernisierung, von Arbeitsverdichtung, von individueller Datenverarbeitung, Workflow-Management und dergleichen. Will man wissen, welche **konkreten Veränderungen und Verbesserungen** von dem geplanten bzw. realisierten Technikeinsatz zu erwarten sind, welche Arbeitsschritte durch welche automatisierten Abläufe ersetzt werden, welche Zuständigkeiten wohin verlagert werden und vor allem welcher Nutzen für die Mitarbeiter, die Behörde und den betroffenen Bürger eintreten soll, erhält man nicht selten nur Hinweise auf noch nicht abgeschlossene Erfahrungsberichte; gelegentlich wird ergänzend auf nicht quantifizierbare Vorteile, auf Sachzwänge, auf die Notwendigkeit, den technischen Anschluß halten zu müssen, und auf die Zuständigkeit anderer zur Beantwortung dieser Fragen hingewiesen.

Eine **Techniklastigkeit** und **Technikgläubigkeit** der Verwaltung bei ihren Bestrebungen, uneffektive Verwaltungsabläufe zu optimieren, ist mithin nicht zu übersehen. Allzu häufig ist das Ziel einer Maßnahme noch gar nicht abschließend definiert, da sind die hard- und software-technischen Komponenten schon geordert. Im weiteren richtet sich nicht die Technik nach den objektiven Erfordernissen, sondern man paßt die Verfahrensweisen so gut es eben geht und soweit rechtlich gerade noch vertretbar den technischen Gegebenheiten an. **Nicht die Technik dient, sie wird bedient.**

Aus vielen Beispielen hierfür seien nur folgende exemplarisch herausgegriffen:

- Im Rahmen des **Personalverwaltungs- und Personalmanagementsystems**, das unter der Federführung des Innenministeriums entwickelt wurde, werden bereits Datenbanken mit Tausenden von Einzelinformationen gefüttert, obwohl man noch gar nicht weiß, wie man bei späteren Auswertungen die Aktualität und Vollständigkeit der Daten gewährleisten kann und wer die Richtigkeit der Selektionsmerkmale testet.

- Nach wie vor werden **Polizeidienststellen** parallel zum COMPAS-Projekt mit **Einzelplatz-PC** ausgerüstet, um einen vermeintlich dringenden Bedarf zu decken. Zu welchen Zwecken die vielen hundert Geräte tatsächlich eingesetzt werden, kann schon längst nicht mehr wirkungsvoll überwacht werden. Die Verpflichtung aus dem Landesverwaltungsgesetz, die Errichtung von Dateien auf das erforderliche Maß zu beschränken, in angemessenen Abständen die Notwendigkeit ihrer Weiterführung zu prüfen und in Errichtungsanordnungen ihre Zweckbestimmung festzulegen, dürfte deshalb kaum erfüllt werden können.

- **Krankenhausinformationssysteme** speichern eine Vielzahl von Patientendaten über lange Zeiträume in Datenbanken und stellen sie über Netzwerke an vielen Arbeitsplätzen bereit, obwohl nach Abschluß und Abrechnung einer stationären Behandlung eine Namenskartei mit einem Verweis auf die papierene Behandlungsdokumentation ausreichen würde.

- In kleinen Organisationseinheiten (z.B. Kommunen) werden **komplexe Client-Server-Konfigurationen** mit mehreren Betriebssystemen installiert, bevor geklärt und getestet wurde, welcher Administrationsaufwand von wem zu erbringen ist, um die erforderliche Verfügbarkeit der Verfahren langfristig zu gewährleisten.

Die Ursache dafür, daß in diesen Fällen das Pferd von hinten aufgezäumt worden ist, liegt nach unseren Erkenntnissen an zu kurzen und zu wenig intensiven Planungsphasen. Die weit überwiegende Mehrzahl der Entscheidungsträger in der öffentlichen Verwaltung sind zwar ausgebildete Verwaltungsrechtler, aber keine IT-Spezialisten. Die Planung und Realisierung von IT-Systemen stellt sich ihnen daher als ein Problem dar, für das anerkannte und bewährte Grundlagen und Entscheidungsmaßstäbe fehlen. Auch die allgemeinen und bereichsspezifischen Vorschriften zur IT-gestützten Datenverarbeitung (vgl. Landesdatenschutzgesetz, Sozialgesetzbuch X, Landesverwaltungsgesetz) setzen für ihre richtige Auslegung ein Mindestmaß an IT-Kenntnissen voraus. Automatisierte Verfahren bestehen nun einmal nicht nur aus dem PC, sondern aus den vier Elementen „Hardware“, „Software“, „Daten“ und vor allen Dingen

der „Orgware". Jedes Element hat vielfältige Beziehungen zu allen anderen. Im Hinblick auf die IT-Planung ist daher jedem von ihnen eine gleichgroße Bedeutung beizumessen. **Planungsfehler** in einem Bereich haben häufig negative Auswirkungen in allen anderen Bereichen. Dabei geht es nicht nur um so vordergründige Probleme, daß zu geringe technische Kapazitäten den Einsatz bestimmter Softwareprodukte unmöglich machen, Mängel in der Datenorganisation zu inkonsistenten Dateien führen oder unzureichende Tests falsche Ergebnisse nach sich ziehen. Als die eigentliche Achillesferse stellt sich in der Praxis die Orgware dar. Wer das Ziel und die Rahmenbedingungen einer IT-Maßnahme nicht klar definiert, kann nicht erwarten, daß die Ergebnisse optimal sind.

Stichwort: Orgware
Mit dem Kunstwort „Orgware" umschreibt man in sprachlicher Anlehnung an Hard- und Software die organisatorischen Rahmenbedingungen und Einzelregelungen, die die Administration und die Benutzung automatisierter Verfahren definieren. Zur Orgware gehören z.B. IT-Konzepte, Sicherheitskonzepte, IT-Dienstanweisungen, Benutzerhandbücher, Aufgabenbeschreibungen, Organisationspläne usw.

Wenn wir derartige **Schwachstellen** bei unseren Prüfungen kritisieren, ist daher nicht zu akzeptieren, daß „der Datenschutz" für die manchmal nicht unerheblichen **„Korrekturkosten"** verantwortlich gemacht wird.

In der Regel gelangen die Diskussionen erst dann wieder in die richtige Richtung, wenn wir Antwort auf die Frage verlangen: „Wären die Sicherheitsrisiken und die rechtlichen Probleme nicht vorhanden, wenn es das Datenschutzrecht nicht gäbe?" (vgl. zu dieser Thematik auch 18. TB, Tz. 6.1 bis 6.3 und 6.7.3 sowie Tz. 6.2 dieses Berichtes).

Was ist zu tun?
Die für den Einsatz von Informationstechnik in der öffentlichen Verwaltung verantwortlichen Entscheidungsträger müssen der Planung automatisierter Verfahren eine größere Bedeutung beimessen und von der Vorstellung abrücken, daß Technik von sich aus die Lösung aller Probleme bringt.

6.2 Der Beratungsbedarf der Kommunen und anderer kleinerer Organisationseinheiten

IT-Konzepte sind als Grundlage für die Realisierungsphase automatisierter Verfahren unverzichtbar. Behörden, die nicht in der Lage sind, derartige Soll-Regelungen zu erstellen, sind auf externe Berater angewiesen. Immer mehr Behörden wollen deshalb die Dienste des Datenschutzbeauftragten in Anspruch nehmen.

Unter Textziffer 1.2 des 18. Tätigkeitsberichtes ist dargestellt worden, in welchem Umfang in den nächsten Jahren von den datenverarbeitenden Stellen im Lande **in Informationstechnik investiert** werden wird. Zu

einem wesentlichen Teil werden diese Investitionen von kleineren Organisationseinheiten mit einem Mitarbeiterstamm zwischen 12 und 20 Personen getätigt. Gleichwohl belaufen sich die Kosten für die Neuinstallation bzw. die Umstellung der bestehenden Hard- und Software auf die neuen Gegebenheiten nicht selten auf Größenordnungen von mehr als 500.000 DM. Selbst bei einem solchen Finanzvolumen verzichten die meisten Behörden auf die Erstellung von **IT-Konzepten** als Grundlage für die Realisierung des Projektes, weil ihnen das Know-how und die personellen Kapazitäten fehlen. Die Einschaltung externer Berater stößt allein schon deshalb auf Schwierigkeiten, weil man sich schwertut, den Beratern die **Zielrichtung** des gewünschten Konzeptes zu erläutern. Behörden, die derartige IT-Konzepte in Auftrag gegeben haben, ohne ihre Wünsche zu konkretisieren, erhielten für viel Geld voluminöse Abhandlungen über IT-Philosophien, Prozessor-Kapazitäten und Netztopologien, aber keine konkreten und unmittelbar umsetzbaren Vorschläge für die **Problemlösungen**.

Wenn wir in dieser Situation um Hilfe gebeten werden, können wir natürlich nicht als Unternehmensberater agieren, dies ist weder unser gesetzlicher Auftrag, noch verfügen wir über die personellen Kapazitäten. Wir schlagen den Behörden jedoch vor, von den externen Beratern bzw. von ihren eigenen „IT-Spezialisten" ein **IT-Konzept** zu verlangen, das wie folgt strukturiert ist:

a) Beschreibung der Möglichkeiten zur **Effizienzsteigerung und Qualitätsverbesserung** durch einen IT-Einsatz, bezogen auf die **konkreten Gegebenheiten** in der betreffenden Behörde.

b) Vorschläge zum Software-Einsatz, um die unter a) genannten Ziele zu erreichen.

c) Vorschläge zur technischen Ausgestaltung der einzelnen Arbeitsplätze unter Berücksichtigung der unter a) und b) gemachten Vorschläge.

d) Ggf. Vorschläge zur Vernetzung der Arbeitsplatzrechner mit Server/n unter Berücksichtigung der tatsächlichen baulichen Gegebenheiten und der sich aus a) bis c) ergebenden Konsequenzen.

e) Ggf. Vorschläge zur technischen Ausgestaltung der Server unter Berücksichtigung der sich aus a) bis d) ergebenden Konsequenzen.

f) Darstellung der aufbau- und ablauforganisatorischen sowie der systemtechnischen Konsequenzen unter der Annahme, daß entsprechend a) bis e) verfahren wird; Fortschreibung des bisherigen Aufgabengliederungsplans (Geschäftsverteilungsplans) unter Berücksichtigung der IT-bedingten Funktionen und Schnittstellen (Hard- und Software-Administration, Verantwortungsverteilung zwischen den Fachabteilungen und der IT-Abteilung sowie evtl. externen Dienstleistern).

g) Vorschläge zur Ausgestaltung von IT-Dienstanweisungen, bezogen auf die konkreten personellen und organisatorischen Gegebenheiten und unter Berücksichtigung der sich aus a) bis f) ergebenden Konsequenzen.

h) Vorschläge zur zeitlichen Realisierung der einzelnen sich aus a) bis f) ergebenden Maßnahmen; Darstellung verschiedener Handlungsalternativen und ihrer Konsequenzen.

i) Entwicklung eines Schulungsplans unter Berücksichtigung der tatsächlichen personellen Situation sowie der Vorschläge zu den aufbau- und ablauforganisatorischen Maßnahmen und des Realisierungsplanes.

j) Darstellung der finanziellen Auswirkungen der Vorschläge und Maßnahmen; Entwurf einer Kosten-Nutzen-Relation.

Unabhängig von der Größe des jeweiligen Vorhabens (von der Einführung eines neuen Sozialhilfeverfahrens in einer kleinen Amtsverwaltung bis hin zur völligen Reorganisation einer großen Stadtverwaltung) führen „handwerklich sauber" erarbeitete Vorschläge für die einzelnen Komplexe zu einer aussagefähigen **Entscheidungsgrundlage** und - wenn es denn so beschlossen wird - zu einer vernünftigen **Soll-Regelung**.

Hinzu kommt ein weiterer wichtiger Aspekt: Ein so gestaltetes IT-Konzept läßt zweifelsfrei erkennen, was gewollt ist. Darauf aufbauend kann in einem **Sicherheitskonzept** relativ einfach dargestellt werden, wie verhindert werden soll, daß alles, **was nicht gewollt ist, auch nicht möglich ist** (vgl. 18. TB, Tz. 6.2). Liegt ein schlüssiges IT-Konzept vor, ist es für uns deshalb auch viel leichter möglich, zu Sicherheitsfragen beratend Stellung zu nehmen.

Der Nutzen einer solchen Beratung spricht sich offenbar zunehmend herum. Unsere hierfür zuständigen Mitarbeiter sind zur Zeit sechs Monate im voraus „ausgebucht".

Was ist zu tun?

Behörden, die in Informationstechniken investieren, sollten von ihren Beratern in sich schlüssige, unmittelbar umsetzbare IT-Konzepte verlangen; dazu müssen sie ihnen aber auch ihre Zielvorstellungen und die rechtlichen Rahmenbedingungen transparent machen.

6.3 Kurswechsel bei der Automationskommission

Selbst sorgfältige Softwaretests schließen Programmfehler nicht aus. Unzureichende und methodisch fragwürdige Prüfungen vor dem Echteinsatz automatisierter Verfahren müssen daher schon fast als grobe Fahrlässigkeit betrachtet werden. Dem will die Automationskommission der kommunalen Landesverbände jetzt Rechnung tragen.

Seit Jahren kritisieren wir die Vorgehensweise beim **Test von Programmen** und automatisierten Verfahren, die im kommunalen Bereich eingesetzt werden (vgl. 13. TB, Tz. 6.3). Zu häufig kommt es vor, daß Software und technische Lösungen eingesetzt werden, die weder den rechtlichen noch den sicherheitstechnischen Anforderungen entsprechen, weil insbesondere die kleineren Organisationseinheiten sich nicht in der Lage sehen, jedes einzelne Produkt detaillierten Tests zu unterziehen. Sie vertrauen auf entsprechende Prüfungen durch die **Automationskommission der kommunalen Landesverbände** und deren Gremien. Aber auch deren Organisationsstrukturen und Kapazitäten waren bisher nicht so ausgelegt, daß eine **wirkungsvolle Kontrolle** der Produkte der am Markt agierenden Softwarehäuser möglich war.

Selbst eine bindende Anweisung des Innenministeriums aus dem Jahre 1990, in dem Bereich des Meldewesens ausschließlich von Melderechtsspezialisten getestete Software einzusetzen, wurde bislang nur sehr eingeschränkt befolgt. Eine Freigabeempfehlung nach entsprechenden Prüfungen durch eine damit beauftragte „Testkommune" wurde für ein Produkt der Datenzentrale erst ausgesprochen, nachdem über 50 Kommunen diese Programme bereits **länger als ein Jahr** in der Praxis einsetzten. Glücklicherweise wurden bei den verspäteten Tests keine gravierenden Fehler entdeckt.

Vor diesem Hintergrund hat die Automationskommission nunmehr „Empfehlungen zur Neufassung der Aufgabenstellung der Automationskommission und ihrer Gremien" sowie „Empfehlungen zum Test und zur Freigabe von IT-Produkten in Kommunen" erarbeitet und der Arbeitsgemeinschaft der kommunalen Landesverbände zur Beschlußfassung vorgelegt.

Die Kommission **folgt damit weitgehend den Vorschlägen**, die wir im Rahmen unserer beratenden Mitarbeit gemacht haben:

- Es sollte grundsätzlich zwischen dem Test von Software und der Freigabe von Verfahren unterschieden werden. In der **Datenschutzverordung** ist nämlich ausdrücklich festgelegt, daß die **Einsatzfreigabe** der automatisierten Verfahren durch die datenverarbeitenden Stellen selbst zu erfolgen hat. Für die Durchführung von **Testarbeiten** können sie

sich dagegen der Unterstützung von Dienstleistern bedienen. Dies kann jedoch nur im Wege der **Auftragserteilung** geschehen, die rechtliche Verantwortung verbleibt bei der Stelle, die das jeweilige Verwaltungsverfahren betreibt.

- Wird Software von einer **Vielzahl von Anwendern** in gleicher Weise eingesetzt, erscheint es nicht ökonomisch, daß jeder zusätzliche Anwender sich erneut davon überzeugt, daß die Programme die zu erwartenden (richtigen) Ergebnisse erbringen. Will man sich jedoch auf die Testergebnisse der bisherigen Anwender **verlassen,** müssen Art und Umfang dieser Tests bekannt und dokumentiert, das Testergebnis schriftlich fixiert und die getesteten Programmversionen exakt bezeichnet sein.

- Bisher bezogen sich die Überlegungen der Kommunen zu dem Problem „Test mit Wirkung für andere" nur auf Software, die von der Datenzentrale entwickelt worden ist. Im Zeichen einer immer breiteren Angebotspalette auch für den kommunalen Bereich erscheint eine solche Begrenzung weder sinnvoll noch erforderlich. Es sollten daher **grundsätzlich alle Anbieter** die Möglichkeit haben, ein anerkanntes Testat für ihre Produkte zu erhalten.

- Die **Initiative** zur Erlangung eines Testats sollte grundsätzlich von dem jeweiligen **Anbieter** ausgehen. Er sollte alle mit dem Test in Zusammenhang stehenden Leistungen zu erbringen und die daraus resultierenden Kosten zu tragen haben.

- Die **Auswahl der Tester** sollte dem Anbieter obliegen. Grundsätzlich sollten mindestens zwei Stellen mit der Durchführung des Tests beauftragt werden. Es sollte sich um Mitglieder der kommunalen Landesverbände handeln. Die Tester sollten nur Verpflichtungen gegenüber dem Anbieter, nicht aber gegenüber der Automationskommission eingehen. Die Vereinbarungen zwischen dem Anbieter und den Testern sollten allerdings schriftlich fixiert sein.

- Vor Durchführung der Tests sollte vom Anbieter ein **Testkonzept** zu enwickeln und mit den Testern und den Gremien der Automationskommission abzustimmen sein. In ihm wären folgende Punkte schriftlich zu fixieren:

  - Gegenstand des Tests (Verfahren, Programme, Versionen),
  - zu beachtende rechtliche Grundlagen,
  - sonstige zu beachtende Vorgaben (z.B. Pflichtenheft, Softwareentwicklungsauftrag, Schnittstellen zu anderen Verfahren, Sicherheitskriterien),
  - Testumgebung (Testsystem, flankierende Software),
  - Testmethoden (Pilotierung, Schattenläufe, Simulation mit Testfällen, Integrationstest),

- Dokumentation der Testfälle, der zu erzielenden Arbeitsergebnisse und der tatsächlichen Ergebnisse,
- Form des Testprotokolls (verbale Beschreibung des Ablaufs, Systemprotokolle, Listen),
- Form des Testats,
- zu beteiligende Institutionen (z.B. Aufsichtsbehörden, Landesbeauftragter für den Datenschutz, Landesrechnungshof, Personalräte).

- Das Testkonzept sollte einen **kontinuierlichen Test von Software** ermöglichen. Für den Fall, daß bei nachfolgenden Tests bisher nicht erkannte Fehler oder Mängel festgestellt werden, wäre zu gewährleisten, daß diese entweder unverzüglich behoben werden oder daß allen beteiligten Institutionen und Anwendern ein modifiziertes **Testat** zugeht. Die Tester sollten gehalten sein, Zweifelsfragen und Testfälle der Anwender in angemessener Zeit zu überprüfen bzw. abzuarbeiten. Sie sollten sich verpflichten, die von ihnen erstellten bzw. dokumentierten Testunterlagen und Testprotokolle nach Ablauf ihrer Tätigkeit ihren Nachfolgern zu übergeben.

- Das Testat sollte hinreichend genau beschreiben, welche Produkte auf welche Weise mit welchem Ergebnis wann von wem getestet worden sind. Es sollte auch Auskunft darüber geben, welche **Rahmenbedingungen** (technische und organisatorische Einsatzvoraussetzungen) der künftige Anwender einzuhalten hat, um das beschriebene Testergebnis zu erzielen. Außerdem wäre sicherzustellen, daß Mängel, die gleichwohl dem positiven Testat nicht entgegengestanden haben, den künftigen Anwendern bekannt werden.

- Bietet ein Anbieter sein Produkt als **„Paketlösung"** (d.h. als integraler Teil eines Hardware-, Software- und Organisationskonzeptes) an, so sollte das Testat auch eine Bewertung dieser Komponenten bzw. Lösungen enthalten (Qualität der Handbücher, Wirksamkeit von Sicherheitsmaßnahmen, Fragen der Systemadministration usw.).

- Das **abschließende Votum** darüber, ob und in welchem Umfang aufgrund des Testats künftige Anwender auf eigene Tests verzichten können, sollte der Automationskommission bzw. ihren Gremien obliegen. Die Beschlußfassung hierüber sollte protokolliert werden. Die Anbieter wären zu unterrichten. Erst **danach** wären sie berechtigt, ihre Software als von den kommunalen Landesverbänden testiert zu bezeichnen.

- Der Anbieter sollte sich verpflichten, jeder Auslieferung an ein Mitglied der kommunalen Landesverbände **das betreffende Testat** beizufügen.

Eine Entscheidung der Arbeitsgemeinschaft der kommunalen Landesverbände stand zum Zeitpunkt des Redaktionsschlusses dieses Berichtes noch aus.

Was ist zu tun?
Die Gremien der „kommunalen Familie" sollten sich konsequent für effektive aufbau- und ablauforganisatorische Maßnahmen im Zusammenhang mit dem Test von IT-Produkten einsetzen. Zum eigenen Nutzen, insbesondere aber zum Nutzen der betroffenen Bürger, sollten die Empfehlungen der Automationskommission kurzfristig in Kraft gesetzt werden.

6.4 Sicherheitsrisiken durch Standardsoftware

Im Gegensatz zur Individualsoftware, die exakt auf die Bedürfnisse des Benutzers zugeschnitten wird, deckt die Standardsoftware, z.B. für Textverarbeitung, Graphik- oder Präsentationserstellung, Tabellenkalkulation oder Datenbankverwaltung meist ein größeres Spektrum an Funktionen ab, als der Anwender eigentlich braucht. Dies ist einer der Gründe, weshalb beim Einsatz von Standardsoftware oft Sicherheitsrisiken entstehen.

Durch eine entsprechende Systemkonfiguration muß technisch gewährleistet sein, daß der Benutzer eines Computersystems nur Aktionen ausführen kann, zu denen er berechtigt ist. Passend für jeden Benutzer müssen die Berechtigungen für den Zugriff auf Programme und Daten sowie für das Ausführen bestimmter Aktionen eingestellt werden. Bietet das vorhandene **Betriebssystem** nicht die Möglichkeit, wirksame **Zugriffsbeschränkungen** zu realisieren, muß zu diesem Zweck zusätzliche Sicherheitssoftware installiert werden.

Anschließend kann man eine auf den Anwender zugeschnittene **Benutzungsoberfläche** entwerfen, die ebenfalls nur die zugelassenen Aktionen ermöglichen und andere Funktionalität gar nicht anbieten soll. Im Gegensatz zu den Zugriffsrechten, die unmittelbar im Betriebssystem verankert sind, ist eine Benutzungsoberfläche allerdings in der Regel nur „aufgesetzt". Der Einsatz von „multifunktionaler" **Standardsoftware** führt leider oft zu **Schwächen** in beiden Bereichen:

- Bei dem Microsoft-Office-Paket läßt sich z.B. zwar die Funktionsauswahl in dem Menü und über Piktogramme relativ frei konfigurieren. Eine Beschränkung kann jedoch durch den Nutzer jederzeit rückgängig gemacht werden, wenn die entsprechende Datei nicht vor Veränderungen geschützt wird.

- Mit der nicht deaktivierbaren Makrosprache steht dem Benutzer eine mächtige Programmiersprache zur Verfügung (vgl. 18. TB, Tz. 6.5). Makroviren, die durch Dokumentenaustausch übertragen werden, sind inzwischen verbreitet, selbst im Bereich der Landesverwaltung. Die Ausführung solcher Makroprogramme ist zwar an die Zugriffsrechte

des Anwenders gebunden, doch entfalten deren destruktive Aktionen außerordentlich gefährliche Wirkungen, wenn sie von Benutzern mit umfassenderen Zugriffsberechtigungen (Systemadministratoren, Dienststellenleitung oder Schreibdienst) aufgerufen werden.

- Die Zugriffsrechte können oft nicht so restriktiv vergeben werden, wie es sinnvoll wäre. Meist funktionieren die Produkte nur dann, wenn der Anwender im Programmverzeichnis, im Verzeichnis mit der Systemsoftware und in einem Druckverzeichnis (Spool) weitreichende Berechtigungen hat. Den Benutzern werden im Interesse eines problemlosen Software-Einsatzes häufig technische „Generalvollmachten" ausgestellt.

- Die meisten Produkte ermöglichen eine Kommunikation oder einen (automatisierbaren) Datenaustausch mit anderen Programmen. Der dadurch erheblich erweiterte Funktionsumfang läßt sich in der Regel nicht ausreichend reduzieren.

- Häufig steht der Quellcode nicht zur Verfügung. Bei Firmen in Quasimonopolstellung basiert ein wesentlicher Marktvorteil gerade auf der fehlenden Dokumentation bestimmter Bereiche, denn dies garantiert, daß nur die eigene Firma paßgenau Erweiterungen und neue Versionen liefern kann. Bücher über „Undocumented Features" sind keine Seltenheit mehr. Durch diese mangelnde Transparenz können „Hintertüren" und Sicherheitslücken vom Benutzer nicht ausgeschlossen werden.

Was ist zu tun?
Die Systemverantwortlichen sollten beobachten, welche Sicherheitslücken bei der von ihnen eingesetzten Software bekannt werden, und sofort Gegenmaßnahmen ergreifen. Generell können nur ausgefeilte Zugriffsrechte das Schlimmste verhindern.

6.5 Geringe Lernbereitschaft bei Führungskräften?

Führungskräfte scheuen sich offenbar vor einer intensiven Auseinandersetzung mit den Fragen des Datenschutzes und der Datensicherheit. Entsprechende Kurse der DATENSCHUTZAKADEMIE werden jedenfalls nicht ausreichend in Anspruch genommen.

Seit Jahren versuchen wir in unseren Beratungsgesprächen und im Rahmen der Prüfungsmaßnahmen den Behörden im Lande deutlich zu machen, daß der Slogan „**Datenschutz und Datensicherheit sind Chefsache!**" eben nicht nur ein Programmsatz ist, sondern die zwingende Konsequenz aus den rechtlichen und sicherheitstechnischen Problemstellungen im Zusammenhang mit der automatisierten (und natürlich

auch der konventionellen) Verarbeitung personenbezogener Daten. Den Entscheidungsträgern in der öffentlichen Verwaltung die einschlägigen Kenntnisse zu vermitteln war deshalb ein wesentlicher Grund für den Aufbau der DATENSCHUTZAKADEMIE. Von Anfang an wird ein dreitägiger **Kursus speziell für Führungskräfte** angeboten. Namhafte Referenten halten Vorträge zu folgenden Themen:

- Risiken der elektronischen Datenverarbeitung für das Persönlichkeitsrecht
- Grundzüge des Bundes- und des Landesdatenschutzgesetzes
- Einführung in das bereichsspezifische Datenschutzrecht
- Technische und organisatorische Maßnahmen zur Datensicherheit
- Revisionsfähigkeit und Ordnungsmäßigkeit der Datenverarbeitung
- Datenschutzverordnung des Landes Schleswig-Holstein
- Koordinierungs- und Normungsbemühungen der IT-Kommission des Landes und der Automationskommission der kommunalen Landesverbände
- Besonderheiten bei der Auftragsdatenverarbeitung
- Grundzüge der Datenschutzregelungen für die Wirtschaft
- Darstellung der Maßnahmen zur Datensicherheit bei der Datenzentrale Schleswig-Holstein
- Praktische Umsetzung des Datenschutzes in den Behörden

Während alle anderen Veranstaltungen gut ausgebucht, teilweise sogar „überlaufen" sind, läßt die Resonanz auf das Angebot gerade bei Führungskräften sehr zu wünschen übrig.

Natürlich haben wir nach Gründen für die **Abstinenz** gesucht. Unisono versicherten die von uns befragten Führungskräfte, daß das Thema wichtig und das Angebot attraktiv sei. Auch hätten die Teilnehmer sich durchweg positiv geäußert. Das Problem sei aber die dreitägige Dauer. Über einen so langen Zeitraum könne man sich wegen der hohenArbeitsbelastung nicht aus dem Tagesgeschäft ausklinken. Tragendes Argument hin, vorgeschobene Ausrede her, wir haben reagiert und bieten ab 1997 weiterhin einen nunmehr aber nur **zweitägigen Kursus für Entscheidungsträger** an. Über die Resonanz werden wir berichten.

Was ist zu tun?
Führungskräften in der öffentlichen Verwaltung sollte die Verantwortung für den IT-Einsatz bei der personenbezogenen Datenverarbeitung erst dann übertragen werden, wenn sie den Nachweis der erforderlichen Sachkunde auf diesem Gebiet erbringen können.

6.6 Ergebnisse von Kontrollen im Bereich der automatisierten Datenverarbeitung

6.6.1 Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung der Kommunen: nicht ohne Beanstandungen

In dem Maße, wie die Anforderungen an die Datenverarbeitung steigen, vergrößern sich die Sicherheitsrisiken. Viele Kommunen sind überfordert, können und wollen sich aber nicht beschränken. Bei unseren Kontrollen sind nach wie vor viele Fehler zu beanstanden.

Die im Jahre 1995 begonnenen **Schwerpunktprüfungen** in Kommunalverwaltungen mittlerer Größe sind konsequent fortgesetzt worden, weil die Ergebnisse und Reaktionen der geprüften Stellen einen dringenden „Bedarf" anzeigen. Die vorgefundenen „Verhältnisse" sprechen für sich und sind denen aus dem Vorjahr (vgl. 18. TB, Tz. 6.7.3) durchaus vergleichbar. Ein Auszug aus den Prüfungsprotokollen:

- Vor dem Echteinsatz von Software wurden **keine Tests** durchgeführt.

- **Softwareänderungen** durch den Anbieter wurden von der Verwaltung übernommen, ohne zu fragen, warum eine Änderung der Programme erforderlich wurde.

- Änderungen an Betriebssystemen, Programmen und Datenbeständen konnten **ohne Protokollierung** vorgenommen werden.

- Die Aktivitäten von externen Dienstleistern (Softwarehäuser, Systemlieferanten) wurden **nicht überwacht** bzw. konnten wegen fehlender Fachkenntnisse gar nicht überwacht werden.

- Die Speicherung von Textdokumenten mit personenbezogenem Inhalt erfolgte **ohne jeden Sinn**, bis die „Platte platzte". Der „Rekord" lag bei 2300 Dokumenten aus drei Jahren, wobei es sich bei den meisten um Schriftverkehr aus dem Sozialamt handelte.

- Mitarbeiter bauten ihre **eigenen Datenbestände** auf, eine Kontrolle fand nicht statt.

- **Vorgesetzte** mit Kontrollverantwortung waren über die tatsächlichen Verfahrensweisen nicht informiert und mangels Know-how auch gar **nicht in der Lage**, ihrer Kontrollpflicht nachzukommen.

- Die **Fernwartungsaktivitäten** externer Dienstleister konnten nicht überprüft werden, weil niemand in den Behörden verstand, „was da abläuft".

- Einzelplatz-PC wurden eingesetzt, **ohne jedwede Maßnahmen** zur Datensicherheit zu ergreifen.

- Es wurde den Normalbenutzern völlig **überflüssige Software** zur Verfügung gestellt (z.B. alle gängigen Computerspiele, WISO-Tips aus der bekannten Fernsehsendung, Hilfen zur Erstellung von Steuererklärungen, aber auch Tools zur Daten- und Systemmanipulation wie XT-Gold und Norton-Commander).

- Es war **undokumentierte Software** verfügbar, die von einem Mitarbeiter erstellt wurde, der längst nicht mehr in der betreffenden Behörde beschäftigt war.

- Es fehlten **schriftliche Anweisungen** für Mitarbeiter, die mit der Systemadministration betraut waren.

Zwei bezeichnende Sachverhalte lassen sich nicht in einem Satz darstellen:

- In einem **Sozialamt** fiel der **Zentralrechner** aus. Im Rahmen der Beseitigung der Störung ergab sich folgender Ablauf:

  - Der zuständige Systembetreuer war zu diesem Zeitpunkt in Urlaub. Eine Vertretung, die über die erforderlichen Kenntnisse verfügte, war nicht greifbar.

  - Der für die Datensicherung zuständige Mitarbeiter des Sozialamtes war seit einigen Tagen krank. Sicherungskopien waren in dieser Zeit nicht angefertigt worden.

  - Die Verwaltung beauftragte eine ortsansässige Servicefirma, den Fehler auf dem Zentralrechner zu beseitigen.

  - Die Firma konnte den Fehler „vor Ort“ nicht finden und brachte den Zentralrechner mit dem gesamten Datenbestand in ihre Werkstatt. Sie stellte dort einen Festplattendefekt fest.

  - Der Rechner wurde daraufhin auf Anweisung der Verwaltung von der Servicefirma an die Auslieferungsfirma übergeben, um noch bestehende Garantieleistungen in Anspruch zu nehmen.

  - Die Garantiezeit war jedoch erloschen, so daß die Lieferfirma den Rechner mit dem Datenbestand wieder zur Servicefirma zurückbrachte.

  - Diese stellte dem Sozialamt ein Ersatzgerät zur Verfügung und generierte hierauf die Daten der letzten Datensicherung.

- Das Sozialamt schloß sodann für zwei Tage seine Türen, um den nicht gesicherten Datenbestand von drei Tagen zu rekonstruieren.

- Nach einigen Tagen wurde der reparierte Rechner von der Servicefirma zurückgeliefert.

- Die Daten wurden sodann vom Ersatzgerät auf den reparierten Rechner übertragen.

  - Das Ersatzgerät wurde mit dem gesamten Datenbestand der Servicefirma übergeben.

  - Sofern diese Firma die Daten noch nicht gelöscht hat, verfügt sie seitdem über den damals aktuellen Bestand an Sozialhilfedaten, Wohngelddaten und den Schriftverkehr des Sozialamtes, insgesamt einige Tausend Datensätze.

- In einem anderen **Sozialamt** fehlten ausreichende und verschließbare Büroschränke, um die **Akten** sachgerecht zu lagern. Deshalb begann man, die Akten auf dem Fußboden zu stapeln. Als der Platz dort nicht mehr ausreichte, wurden die Fensterbänke belegt. Da die Fenster im Erdgeschoß des Gebäudes aber vom Bürgersteig aus einsehbar waren, dachte man sich eine „hochwirksame" Sicherheitsmaßnahme aus. Die Akten wurden umgedreht, so daß die Namen der Sozialhilfeempfänger von der Straße aus nicht erkennbar waren.

Wie reagierten die geprüften Stellen auf diese Feststellungen? **In keinem einzigen Fall wurde den Beanstandungen widersprochen.** Im Gegenteil, man bat uns um eine eingehende **Beratung,** um die Mängel abzustellen. Allerdings ließ das Tempo der **Abarbeitung der Probleme** in dem Maße nach, wie sich der „Schock" über die vielen Beanstandungen legte. Zitat eines Bürgermeisters: „Es ist erforderlich, daß eine völlig neue Konzeption für die Datenverarbeitung erstellt wird, die sämtliche Bereiche der Verwaltung erfaßt. Die Erstellung dieser Konzeption wird durch den Organisator erfolgen. Da es sich hierbei um eine sehr zeitintensive Aufgabe handelt und der Mitarbeiter lediglich zu 50 Prozent seiner Tätigkeit Aufgaben der Datenverarbeitung wahrnimmt, kann eine fertige Konzeption frühestens ... vorgelegt werden."

Daneben waren weiterhin Beanstandungen im Zusammenhang mit der von der Datenzentrale vertriebenen **MOSAIK-Software,** insbesondere bezüglich des **Finanzinformationssystems,** auszusprechen. Die im 18. Tätigkeitsbericht (vgl. Tz. 6.7.3) dargestellten Rechts- und Sicherheitsprobleme bestehen nach wie vor fort. Zur Erinnerung: Es ging um

- unzureichende Zugriffsbeschränkungen,
- mangelnde Abschottung der Administrationsebene,
- fehlende Tests und Freigabeempfehlungen,

- unzureichende Überwachung von Fernwartungen,
- fehlende Sicherheitskonzepte.

Die **Absicht** der Datenzentrale, diese Lücken im Verlaufe des Jahres 1996 zu schließen, wurde bis Redaktionsschluß offenbar **nicht in die Tat umgesetzt**. Auf Anfrage teilte sie mit, man habe zunächst ein Konzept erarbeitet, das vorsah, die Vergabe der Zugriffsrechte auf Haushaltsstellen auszudehnen. Bei der Realisierung habe sich ergeben, daß die notwendige Definition von gesonderten Gruppenrechten bei den jeweiligen Kundenverwaltungen einen auch aus deren Sicht unverhältnismäßig hohen Administrationsaufwand zur Folge gehabt hätte. Deshalb mußte ein anderer Weg beschritten werden. Außerdem sei die Selektionslogik für die Anzeige der Haushaltsstellen anzupassen und auch der Bereich der Haushaltsüberwachung in den Zugriffsschutz einzubeziehen gewesen. Dies habe einen **beträchtlichen** Aufwand verursacht, da die Änderungen und Erweiterungen **nachträglich** in das bereits im Prinzip fertige Verfahren integriert werden mußten. Man habe daher nicht die gesamte neue Funktionalität zur Verfügung stellen können. Dies werde in **1997 nachgeholt**.

Da wir nicht nur die Zugriffsbeschränkungen in der Teilanwendung „Finanzinformationssystem" als problematisch erachten, und bei Prüfungen nur schwer zu erkennen ist, welche der von der Datenzentrale angebotenen Funktionen vom Kunden nicht genutzt werden, haben wir den Beteiligten eine Art **„Musterprüfung MOSAIK"** angeboten. Wir hoffen, daß die Datenzentrale und einer ihrer Kunden die Hardware-, Software- und Organisationskonzepte des MOSAIK einmal in der optimalen Weise umsetzen, um feststellen zu können, ob auch dann noch datenschutzrechtliche Defizite bestehen.

Was ist zu tun?
Die Kommunalaufsicht, die kommunalen Landesverbände, die Datenzentrale und die anderen IT-Dienstleister sollten sich an einen Tisch setzen und Musterlösungen für den kommunalen Bereich erarbeiten.

6.6.2 Zum Stellenwert des Patientengeheimnisses in einem Krankenhaus

Der Inhalt medizinischer Unterlagen unterliegt einem besonderen Berufsgeheimnis. Da muß man erwarten, daß gerade ein Krankenhaus in öffentlicher Trägerschaft auch besondere Sicherungsmaßnahmen ergreift. Eine datenschutzrechtliche Überprüfung zeigte vielfältige Mängel auf.

Wann immer man ein Beispiel für den „traditionellen" Datenschutz sucht, wird das **Arztgeheimnis**, genauer das **Patientengeheimnis,** angeführt. Geradezu selbstverständlich ist die Annahme, daß persönliche

Dinge, die man einem Arzt anvertraut, anderen Personen oder Stellen nicht zur Kenntnis gelangen. Jede öffentlich bekanntwerdende Gefährdung dieses „Rechtsgutes von höchstem emotionalen Rang" führt zu heftigen Reaktionen. Aus diesem Grunde richten auch wir seit geraumer Zeit unser besonderes Augenmerk auf die Datenverarbeitung durch die Ärzte und die Verwaltungsstellen der **Krankenhäuser in öffentlicher Trägerschaft** (niedergelassene Ärzte und Privatkliniken unterliegen nicht unserer Kontrolle). Nach Prüfungen in Universitätskliniken und ersten Prüfungen in Kreiskrankenhäusern (vgl. 16. TB, Tz. 6.6.4 und 18. TB, Tz. 6.7.2) haben wir das „Programm" auf der Ebene der kommunalen Krankenhäuser fortgesetzt.

Das Kreiskrankenhaus in Elmshorn, eines von vier Krankenhäusern eines **Eigenbetriebes des Kreises** Pinneberg, steht kurz davor, eine psychiatrische Abteilung zu eröffnen. Da traf es sich gut, die automatisierte Datenverarbeitung einem „Sicherheitscheck" zu unterziehen, bevor dort die Computer auch in einem der sensibelsten Bereiche der Krankenversorgung eingesetzt werden.

Zu unserer Überraschung mußten wir feststellen, daß trotz der Größe des Eigenbetriebes (die Kapazität liegt bei ca. 900 Betten) keine verbindlichen Regelungen zur Gestaltung des Einsatzes von Informationstechnik erlassen worden sind. Mithin war eine systematische Analyse und Bewertung der „Soll-Regelungen" sowie ein „Soll-Ist-Vergleich" nicht möglich. Die tatsächlich vorgefundenen Verfahrensweisen mußten daher als „von den Verantwortlichen so gewollt" interpretiert werden. Da auch kein **Sicherheitskonzept** vorgelegt werden konnte, wurde zur Ermittlung eines Maßstabes zur Beurteilung der Maßnahmen in bezug auf die automatisierten Verfahren die Prüfung auf die papierene **Behandlungsdokumentation** ausgedehnt. Dieser Versuch erwies sich als ein „Volltreffer", weil eine Vielzahl von **Unzulänglichkeiten** zutage traten. Die Behandlung der Akten war aus folgenden Gründen ganz und gar nicht vorbildlich:

- Die Verantwortung für das Archiv lag beim Verwaltungsdirektor, genutzt wurde es jedoch fast ausschließlich vom ärztlichen Bereich. Die Herausgabe von Akten wurde zwar registriert. Kamen sie allerdings nicht zurück, waren die Archivmitarbeiter machtlos. Zum Zeitpunkt der Prüfung war eine große Anzahl von Akten trotz mehrmaliger Mahnung auch mehrere Monate nach der Ausgabe noch nicht wieder an das Archiv zurückgegeben worden. Es konnte mithin nicht ausgeschlossen werden, daß sie „**verschwunden**" sind.

- Die Archivmitarbeiter waren auch während der Dienstzeit **nicht ständig** im Archiv anwesend.

- Bei Abwesenheit blieb die Eingangstür **unverschlossen**, da der Zugang zu einem Fax-Gerät, zu dem auf dem Flur gelagerten Kopier-

papier und den Röntgenunterlagen, die von den Mitarbeitern des ärztlichen Bereichs selbst dem Archiv entnommen und zugeführt wurden, gewährleistet sein mußte.

- Unser Prüfer hat sich über einen längeren Zeitraum **unkontrolliert** in einem Archivraum aufhalten können, während mehrere Personen das Archiv betraten und wieder verließen, zeitweilig hat er sich völlig allein im Archiv aufgehalten.

- Auch wenn das Archivpersonal anwesend war, konnte es das „Kommen und Gehen" wegen der Verteilung der Akten auf mehrere Räume nicht überwachen. Die gezielte **unbefugte Entnahme** von Akten, eine Auswertung außerhalb des Archivs und eine Rückführung nach mehreren Tagen wäre nicht aufgefallen.

- Teilweise wurden Akten auf dem Weg in den ärztlichen Bereich in sogenannten Postfächern zwischengelagert. Diese Fächer waren **allgemein zugänglich**.

Diesem zweifelsfrei zu niedrigen Sicherheitsniveau vergleichbar waren auch die Sicherungsmaßnahmen bezüglich der **automatisierten Verfahren**. Es wurden von uns daher u.a. folgende Sachverhalte beanstandet:

- Für jeden stationär aufgenommenen Patienten wurde parallel zur papierenen Dokumentation in einer Datenbank ein **Stammsatz** angelegt, der u.a. folgende Merkmale enthielt: Name, Vorname, Anschrift, Familienstand, Konfession, Staatsangehörigkeit, Beruf, Diagnosen, Befunde, Abrechnungsdaten, Angehörige, Arbeitgeber. Die Datensätze wurden auch nach Abschluß der Behandlung und Abrechnung der Kosten **nicht gelöscht**. Zu welchen Zwecken die Daten auf Dauer gespeichert wurden, konnte im Rahmen der Prüfung nicht abschließend geklärt werden.

- Allen Mitarbeitern der **Systemadministration** (also auch den Mitarbeitern des externen Softwarehauses) war jederzeit ein **undokumentierter Zugriff** auf alle Stammdatensätze möglich. Das galt z.B. auch für die Daten der Patienten der Belegärzte und der Personen, die zum Zwecke der ärztlichen Begutachtung stationär aufgenommen wurden.

- Systematische Tests mit speziellen Testdaten zur Überprüfung der fachlichen Richtigkeit der Verfahren wurden nicht durchgeführt. Die **Echtdaten** wurden auch zu **Testzwecken** genutzt. Da allein in den letzten neun Monaten vor der Prüfung 34 Änderungen an der Software vorgenommen wurden, muß von einem permanenten Test mit Echtdaten ausgegangen werden.

- Die Zuständigkeiten für die **Freigabe** der Hard- und Software zum Echteinsatz waren **nicht eindeutig** geregelt. De facto wurden die Entscheidungen von den Systemadministratoren getroffen. Sie agierten insoweit in einem „revisionsfreien" Raum.

- Die vorhandenen **Dokumentationsunterlagen** waren **nicht geeignet**, die Verfahrensspezifikationen für einen sachverständigen Dritten nachvollziehbar zu machen.

- Die **Zugriffsbefugnisse** auf die Patientenstammdaten waren **nicht restriktiv** genug gestaltet. So wurden z.B. dem Pförtnerdienst die Identitätsdaten, die Staatsangehörigkeit, die Konfession, der Familienstand und der Arbeitgeber aller Patienten, die in den letzten drei Jahren behandelt worden sind, angezeigt. Tatsächlich benötigte der Pförtnerdienst nur die Merkmale: Name, Vorname und Station der zum jeweiligen Zeitpunkt stationär aufgenommenen Patienten.

- Die Benutzung von 20 unvernetzten Arbeitsplatzrechnern unterlag **keinen sicherheitstechnischen Restriktionen**. Teilweise war ein Paßwortschutz realisiert, der allerdings dazu führte, daß selbst Vorgesetzte nicht die Möglichkeit hatten, sich einen Überblick über die gespeicherten Daten zu verschaffen. In diesem Bereich wurden überwiegend Personaldaten verarbeitet.

Wir haben eine Reihe von **Beanstandungen** ausgesprochen und dem Kreis als dem Träger des Krankenhauses sowie der Geschäftsführung des Eigenbetriebes und der Krankenhausleitung in einem Zehn-Punkte-Katalog Vorschläge zur Verbesserung des Datenschutzes gemacht.

In einer ersten Stellungnahme hat die Geschäftsführung des Krankenhauses angekündigt, das Archiv künftig in die Verantwortung des ärztlichen Direktors zu übergeben. Über die Löschungsfristen für die Patientenstammsätze in dem Klinikinformationssystem konnte noch kein Einvernehmen erzielt werden. Hierüber sowie über die weiteren Beanstandungen, denen im Grundsatz nicht widersprochen wurde, sind wir zwischenzeitlich in die Beratungsphase eingetreten, in der wir das Krankenhaus bei der praktischen Umsetzung unterstützen.

6.6.3 Disziplinarverfahren auf PC vergessen

Bei der Kontrolle der EDV-Anwendungen in einer Krankenkasse fanden wir im wesentlichen vernetzte PC mit eigenen Festplatten. Auf einem dieser Geräte wurden bei einer Stichprobenkontrolle mehrere Texte gefunden, die nicht aus dieser Abteilung stammen konnten. Unter anderem handelte es sich um eine Sitzungsvorlage, die **disziplinarische Ermittlungen** gegen einen Mitarbeiter zum Gegenstand hatten. Es ging dabei um den Vorwurf der sexuellen Belästigung am Arbeitsplatz. Weiter fanden sich ein Schreiben in einer Widerspruchsangelegenheit sowie Aufstellungen über Wochenüberstunden anderer Mitarbeiter.

Uns wurde hierzu erklärt, das Gerät sei vor seinem Einsatz bereits in anderen Abteilungen verwandt worden. Offenbar seien die Texte bei der Übergabe versehentlich nicht gelöscht worden. Nach unserer Beanstandung wurde dies unverzüglich nachgeholt.

7. Neue Medien und Informationstechniken

7.1 Multimedia

Besonders im Unterhaltungsmarkt nimmt Multimedia immer mehr Raum ein. Über Satellit oder Kabel geht das digitale Fernsehen auf Sendung. Dabei dürfen die Interessen und Sehgewohnheiten der Zuschauer nicht gespeichert werden.

Beim digitalen Fernsehen ist für den Kunden vor allem die Möglichkeit neu, nur für die Programmangebote zu bezahlen, die auch wirklich gesehen wurden. Diese **Pay-per-View-Angebote** werden grundsätzlich verschlüsselt übertragen und müssen für den Empfang dekodiert werden. Hierzu benötigt man eine sogenannte Set-Top-Box, in die der Kunde seine Chipkarte einführt. Für die Freischaltung werden zur Zeit verschiedene technische Verfahren eingesetzt:

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

- Bei der **zentralen Freischaltung** muß der Kunde zunächst dem Sender mitteilen, welche Sendung er sehen möchte. Zusammen mit dem Sendesignal werden dann die Nutzernummern der Interessenten unverschlüsselt übertragen, deren Decoder freigeschaltet werden soll.

- Für die **lokale Freischaltung** durch den Nutzer wird jede Sendung mit einer elektronischen Entgeltinformation (Token) gekoppelt. Die an einer Sendung interessierten Kunden geben ihren Wunsch mit der Fernbedienung an ihre Set-Top-Box weiter, die die Kosten für das Programmangebot von der Guthaben-Chipkarte im Decoder abbucht und die Sendung freischaltet.

Während bei der zentralen Freischaltung das vom Kunden gewünschte Programmangebot zu Abrechnungszwecken beim Sender gespeichert wird und durch die unverschlüsselte Übertragung der Nutzernummern sogar im gesamten Netz mit geringem Aufwand ausgewertet werden kann, braucht der Kunde bei der lokalen Freischaltung keine personenbezogenen Daten aus der Hand zu geben.

Nach Aussage der Veranstalter drängen die Programmlieferanten und internationalen Inhaber von Senderechten auf eine genauereAbrechnung. Nach unserer Auffassung entsteht daher die Gefahr, daß die persönlichen **Vorlieben, Interessen** und **Sehgewohnheiten** der Zuschauer **registriert**

werden. Deshalb fordern wir gemeinsam mit den anderen Datenschutzbeauftragten des Bundes und der Länder, daß solche Freischaltungsverfahren angeboten werden, bei denen sich die Nutzung der Programmangebote nicht personenbezogen speichern läßt. Nur so kann dem transparenten Verbraucher vorgebeugt werden. Dies ist in den Entwürfen für den Mediendienste-Staatsvertrag und das Teledienstegesetz bislang auch vorgesehen (vgl. Tz. 7.2).

Was ist zu tun?
Gerade im Multimedia-Bereich sollten die neuen Nutzungs- und Abrechnungsformen datenschutzgerecht gestaltet werden. Die technischen Voraussetzungen dafür sind gegeben.

7.2 Gesetzentwürfe zum Multimedia-Bereich

Mitte 1997 sollen die Regelungen zu Tele- und Mediendiensten in Kraft treten. Wegen der unterschiedlichen Regelungskompetenzen von Bund und Ländern sind zwei Gesetze notwendig: Der Bund hat das Informations- und Kommunikationsdienstegesetz (IuKDG) vorbereitet, die Länder streben einen Mediendienste-Staatsvertrag (MDStV) an.

Die Datenschutzregelungen des Bundes sind im Artikel 2 des IuKDG zum eigenständigen **Teledienstedatenschutzgesetz** (TDDSG) zusammengefaßt; der Staatsvertrag der Länder soll gleichlautende Bestimmungen enthalten. Erstmals in einem deutschen Gesetz soll hier der **Grundsatz der Datensparsamkeit** festgeschrieben werden: Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.

> ***Stichwort: Teledienste***
> *Bei Telediensten steht die individuelle Nutzung im Vordergrund, wodurch sich die Regelungskompetenz des Bundes ergibt.*
> *Beispiele: elektronischer Datenaustausch, Videokonferenzen, Internet, Online-Dienste, elektronische Buchungen, Telebanking, Telearbeit, Telemedizin, Telespiele.*

Außerdem sollen die Diensteanbieter verpflichtet werden, den Nutzern, soweit technisch möglich, die Inanspruchnahme von Diensten und ihre Bezahlung **anonym** oder unter **Pseudonymen** zu ermöglichen. Nutzungsprofile sollen nur bei der Verwendung von Pseudonymen zulässig sein und dürfen nicht mit den Daten über den Träger des Pseudonyms zusammengeführt werden. Problematisch ist derzeit noch die Gestaltung der Pseudonyme. Die Anbieter sehen bereits eine von ihnen vergebene Nummer auf einer Chipkarte als Pseudonym im Sinne des Gesetzentwurfs an. Hier ist der Personenbezug jedoch leicht wieder

herstellbar. Dabei wird es in vielen Fällen selbst für Direktwerbezwecke gar nicht erforderlich sein, den Namen des Trägers eines Pseudonyms zu kennen. Beispielsweise könnte bei Pay-per-View (vgl. Tz. 7.1) mit Hilfe der Nutzungsdaten auf die Interessen der Teilnehmer geschlossen und gezielt entsprechende Werbung eingespielt werden, ohne daß Name und Adresse des Nutzers bekannt sein müssen. Deshalb sollte das Pseudonym so gewählt sein, daß die Identität des Betroffenen auch vom Anbieter nicht erkennbar ist.

Wie auch im Telekommunikationsgesetz und Signaturgesetz (vgl. Tz. 7.7) wird der **Zugriff der Sicherheitsbehörden** auf personenbezogene Daten ermöglicht, die für die Begründung, Ausgestaltung oder Änderung eines Vertragverhältnisses erhoben sind (Bestandsdaten). Zu kritisieren ist, daß man bis jetzt weder eine Protokollierung dieser Datenübermittlung noch eine Information des Betroffenen wenigstens im nachhinein vorgesehen hat und daß nicht nur die Strafverfolgungsbehörden, sondern auch die Geheimdienste in den Kreis der Abfragenden aufgenommen wurden.

Stichwort: Mediendienste
Mediendienste sind an die Allgemeinheit gerichtet und bestehen aus Verteil- und Abrufdiensten. Wie auch der Rundfunk unterliegen sie der Regelungskompetenz der Länder, da die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht.
Beispiele: Pay-TV, elektronische Presse, Teletext. Strittig ist die Zuordnung der Dienste Teleshopping oder Video-on-Demand.

Ob es nach Teledienstedatenschutzgesetz und Mediendienste-Staatsvertrag eine **einheitliche Datenschutzkontrolle**, z.B. beim Bundesbeauftragten für den Datenschutz, geben wird, ist noch unklar. Leider ist man inzwischen wieder davon abgerückt, ein Datenschutz-Audit verbindlich vorzuschreiben.

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

Was ist zu tun?
Der Datenschutz der Kunden sollte in den Gesetzentwürfen nicht mehr verwässert, sondern in einigen Punkten noch verbessert werden.

Überblick über das Telekommunikations- und Medienrecht

Rundfunk-Staatsvertrag der Länder (1991) in Schleswig-Holstein zusätzlich: **Landesrundfunkgesetz (1995)** regelt: Rundfunk Fernsehen	**Mediendienste-Staatsvertrag der Länder (voraussichtl. ab Mitte 1997)** regelt z.B.: Pay-TV elektron. Presse Teletext	**Teledienstegesetz mit Teledienstedatenschutzgesetz des Bundes (voraussichtl. ab Mitte 1997)** regelt z.B.: Telebanking Telearbeit Telemedizin Telespiele Online-Dienste Internet Videokonferenzen
	Einordnung strittig: Teleshopping Video-on-Demand	
Telekommunikationsgesetz des Bundes (August 1996)	regelt: Telefonate Faxe Mobilfunk Datenfernübertragung Electronic Mail Netzzugänge Telekommunikation als Basis von Medien und Telediensten	

7.3 Neue Gesetze regeln die Telekommunikation

Die Telekommunikation ist eine Schlüsseltechnologie der Informationsgesellschaft und somit ein entscheidender Wirtschaftsfaktor. Aus diesem Grund liegt hier zur Zeit ein Schwerpunkt der Gesetzgebung. Neu sind das Telekommunikationsgesetz und die Telekommunikationsdienstunternehmen-Datenschutzverordnung.

7.3.1 Telekommunikationsgesetz

Die Postreform ebnet den Weg vom ehemals staatlichen Monopol im Telekommunikationssektor zum **freien Markt**, der ab 1998 in der ganzen Europäischen Union bestehen wird. Die rechtliche Ausgestaltung legt das neue Telekommunikationsgesetz (TKG) fest, das am 1. August 1996 in Kraft getreten ist. Zweck des Gesetzes ist es, durch Regulierung des Tele-

kommunikationsbereichs den Wettbewerb zu fördern und eine flächendeckende Grundversorgung zu gewährleisten. Dabei geht es nicht nur um den Sprachtelefondienst, sondern auch um Datenübertragung, z.B. in Form von elektronischer Post (E-Mail).

Aufsehen erregte eine Bestimmung, nach der die Netzbetreiber verpflichtet werden sollten, längere Zeit zu speichern, wer mit wem wann wie lange telefoniert hat. Schließlich hätten die weitreichenden **Zugriffsbefugnisse von Sicherheitsbehörden** nur Sinn, wenn auch genügend Daten verfügbar seien, wurde argumentiert. Gegen diesen Schritt in den Überwachungsstaat haben wir uns vehement gewandt. Auch unverdächtigte Bürger hätten nämlich damit rechnen müssen, daß ihr Telefonierverhalten jederzeit Gegenstand von lautlosen Rasterfahndungen geworden wäre. Die Landesregierung unterstützte die datenschutzrechtlichen Bedenken im Bundesrat. Dies dürfte dazu beigetragen haben, daß der umstrittene „Mindestfristen-Passus" wieder gestrichen wurde.

Stichwort: Telekommunikation
Kommunikation zwischen Menschen, Maschinen und anderen Systemen mit Hilfe von nachrichtentechnischen Übertragungsverfahren. Telekommunikation liegt Telefonaten und Mobilfunk ebenso zugrunde wie Fernsehen, Rundfunk oder Datenübertragung in Computernetzen.

Für den Telefonkunden finden sich im Gesetz einige **begrüßenswerte Regelungen**:

- Auch nichtkommerzielle Anbieter werden zur Wahrung des **Fernmeldegeheimnisses** verpflichtet. Es umfaßt neben dem Inhalt der Telekommunikation auch die Informationen über die Verbindung oder Verbindungsversuche. Leider fehlt eine Sanktionsregelung. Angesichts der Grundrechtsrelevanz der vertraulichen Telekommunikation wäre eine besondere Strafvorschrift unserer Ansicht nach geboten gewesen.

- Die **Sicherheit der Telekommunikationseinrichtungen** wird großgeschrieben. Jeder Betreiber ist verpflichtet, z.B. technische Maßnahmen zur Datensicherheit und speziell zum Schutz personenbezogener Daten zu treffen.

- In einer noch zu erlassenden **Rechtsverordnung** müssen weitere Details des Datenschutzes geregelt werden. Die Eckpunkte werden allerdings schon im Gesetz vorgegeben, z.B. die Beschränkung der Datenerhebung, -verarbeitung und -nutzung auf das Erforderliche und der Grundsatz der Zweckbindung. Personenbezogene Daten dürfen für Werbung, Kundenberatung, Marktforschung, in öffentlichen gedruckten oder elektronischen Verzeichnissen oder bei einem Auskunftsdienst nur mit **Einwilligung des Kunden** verwendet werden. Sofern die Daten zu diesen Zwecken bereits vor Inkrafttreten des neuen

Gesetzes genutzt wurden, gilt das Einverständnis des Kunden als erteilt, wenn er in angemessener Weise über sein Widerspruchsrecht informiert worden ist und von seinem Widerspruchsrecht keinen Gebrauch gemacht hat.

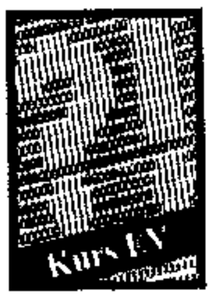
- Für den gesamten Bereich der Telekommunikation haben die Bürger **einen Ansprechpartner**, den Bundesbeauftragten für den Datenschutz.

Ziel des Gesetzes ist es aber auch, die **Interessen der Sicherheitsbehörden** zu wahren. Sie haben entsprechend weitreichende Befugnisse:

- Auf Ersuchen müssen ihnen die Betreiber diejenigen **Daten** übermitteln, die sie im Rahmen von **Verträgen** mit ihren Kunden erhoben haben, soweit dies zur Strafverfolgung, Gefahrenabwehr oder Aufgabenerfüllung der Geheimdienste erforderlich ist. Aus solchen Vertragsinformationen lassen sich unter Umständen detaillierte Erkenntnisse über Konsum- und Kommunikationsverhalten gewinnen. Beispielsweise könnte man bei Abonnementdiensten auf die Interessen des Kunden schließen. Sie werden überdies nicht über die Auskünfte an Sicherheitsbehörden informiert. Eine Protokollierung der Datenübermittlung zur Datenschutzkontrolle ist ebenfalls nicht vorgesehen.

- Außerdem müssen **Kundendateien** geführt werden, die Name, Anschrift und Rufnummer enthalten. Diese Kundendateien müssen so bereitgestellt werden, daß einzelne Daten oder Datensätze auf Ersuchen der Sicherheitsbehörden automatisiert abgerufen werden können. Die Abrufe werden zentral von der **Regulierungsbehörde für Telekommunikation** und der Telekom vorgenommen. Die Betreiber haben durch technische und organisatorische Maßnahmen sicherzustellen, daß ihnen solche Abrufe nicht zur Kenntnis gelangen können. Dieser **unbeobachtbare Zugang** erzeugt nicht nur ein Unbehagen bei den Datenschützern, sondern lädt auch geradezu zum Mißbrauch ein. Kein Betreiber kann unter diesen Umständen den Schutz seiner Kundendaten gewährleisten, da er einen unbefugten Zugang nicht einmal bemerken könnte. Interessenten für Informationen aus solchen Kundendateien gibt es viele, beispielsweise Wirtschaftsunternehmen, die sich einen Überblick über den gesamten Kundenstamm der Konkurrenz machen wollen. Darüber hinaus enthalten Kundendateien nicht nur bereits

Stichwort: Regulierungsbehörde für Telekommunikation und Post
Ab 1998 wird die Regulierungsbehörde die Einhaltung des Telekommunikationsgesetzes überwachen und für die Lizenzvergabe zuständig sein. Die neue Bundesoberbehörde wird im Geschäftsbereich des Bundesministeriums für Wirtschaft errichtet. Nach dem Signaturgesetz (vgl. Tz. 7.7) soll die Regulierungsbehörde außerdem als oberste Zertifizierungsstelle tätig werden und die Einhaltung der gesetzlichen Regelungen in diesem Bereich kontrollieren.



veröffentlichte Daten, sondern auch Geheimnummern, deren Ausspähung sogar eine Gefahr für Leib und Leben bedeuten könnte, z.B. bei verfolgten Ehepartnern, hohen Funktionsträgern aus Wirtschaft, Politik oder Verwaltung, Prominenten oder Kronzeugen. Noch stehen Details zum Abrufverfahren nicht fest, doch ein Mißbrauch läßt sich keinesfalls ausschließen.

- Die Betreiber müssen den Sicherheitsbehörden die technischen Einrichtungen zur gesetzlich vorgesehenen Überwachung der Telekommunikation zudem kostenlos bereitstellen.

7.3.2 Telekommunikationsdienstunternehmen-Datenschutzverordnung

Knapp zwei Wochen vor dem Telekommunikationsgesetz trat eine Neufassung der Datenschutzverordnung für diesen Bereich in Kraft. Allerdings beruht sie noch auf dem Postregulierungsgesetz von 1994. Kein Wunder, daß es einige Widersprüche zwischen Gesetz und Verordnung gibt. In diesen Fällen geht das neuere Gesetz der älteren Verordnung vor.

Für große Verwirrung hat die sogenannte **Komfortauskunft** gesorgt, bei der nicht nur die Nummer, sondern auch die Adresse, die Berufsbezeichnung und der Titel abgefragt werden können. Während früher der Wohnort des gesuchten Teilnehmers bekannt sein mußte, weil im jeweiligen Telefonbuch gesucht wurde, wird nun im bundesweiten Gesamtbestand recherchiert.

Nach der Datenschutzverordnung dürfen über die Rufnummer hinausgehende Auskünfte nur erteilt werden, wenn der **Kunde** damit **einverstanden** ist. Sein Einverständnis gilt als erteilt, wenn er über sein Wahlrecht informiert wird und nicht innerhalb von vier Wochen Widerspruch einlegt. Die Telekom verschickte daraufhin im August mit den Fernmelderechnungen Informationsblätter über die Komfortauskunft. Wegen ihrer irreführenden Aufmachung wurde die vermeintliche Werbeschrift von vielen Kunden ungelesen weggeworfen. Die Vermischung mit der Widerspruchsmöglichkeit bei öffentlichen Verzeichnissen (vgl. Tz. 7.4) trug zur weiteren Verunsicherung bei. Weitere Beschwerden bezogen sich auf die Beantwortungsfrist von vier Wochen, die gerade in der Ferienzeit von vielen nicht einzuhalten war.

Auf die Kritik der Datenschutzbeauftragten hat die **Telekom** reagiert und einen neuen Prospekt verschickt, in dem sie zugesteht, daß jederzeit Widerspruch sowohl gegen die Aufnahme der Daten in die Komfortauskunft als auch in elektronischen Verzeichnisse möglich ist.

Was ist zu tun?

Es ist darauf zu achten, daß in den künftigen Verordnungen ein hinreichend hohes Datenschutzniveau festgeschrieben wird.

7.4 Telefonverzeichnisse auf CD-ROM

Telefonverzeichnisse auf CD-ROM bieten Nutzungsmöglichkeiten, die über herkömmliche Telefonbücher weit hinausgehen. Sie sind nur zulässig, wenn die Betroffenen nach Aufklärung nicht widersprochen haben. Einige Firmen scheren sich weder um Gesetze noch Gerichtsurteile und vertreiben die CDs weiter.

*„Und es gibt sie doch. Ab sofort ist sie im Handel: Als dritte Version der berühmten Telefon- und Adreß-CD-ROM tritt die **D-Info 3.0** ... mit verbesserter Datenaktualität, zusätzlichen Features und einem fast vorprogrammierten Rechtsstreit in die Fußstapfen ihrer berühmten Vorgängerinnen. ... Sie hat einiges zu bieten: 34 Millionen brandaktuelle Datensätze mit Namen, Telefonnummern und Adressen samt Postleitzahlen, eine Vielzahl verschiedener Such- und Datenselektionsmöglichkeiten auch bei unvollständigen Angaben und anhand von Stichworten. ... Wie von ... gewohnt, liefert die D-Info 3.0 alles, was der Anwender, egal ob geschäftlich oder privat, benötigt. Neu bei dieser Version sind mikrogeografische Daten, die anhand von Straßenstatistiken Informationen über die Infrastruktur der einzelnen Straßen geben: So erfahren Sie, ob der von Ihnen gesuchte Anschluß in einem luxuriösen Einzelwohnhaus, einem riesigen Hochhaus oder mitten im Gewerbegebiet liegt. Es bleibt Ihnen überlassen, hieraus die für Sie wichtigen Schlüsse zu ziehen."*

Soweit die Werbung für eine bekannte CD-ROM mit Telefonbuchdaten. Ebenso wie die Telekom als Telefonunternehmen geben inzwischen mehrere Firmen die **Telefonbücher** elektronisch auf **CD-ROM** heraus. Während die Telekom diese Daten über die eigenen Kunden in ihren Datenbanken gespeichert hat, lassen andere Firmen die 100.000 Seiten der 135 deutschen Telefonbücher beispielsweise in China abtippen.

Stichwort: Telefon-CD-ROM

Ein „elektronisches Telefonbuch" auf CD-ROM oder in allgemein abfragbaren Datenbanken bietet mehr Funktionalität als das Papierwerk, z.B.

- *die Möglichkeit, Telefonteilnehmer überregional - auch ohne Kenntnis des Wohnortes - aufzuspüren,*
- *die Möglichkeit, zu einer Rufnummer Name und Adresse des Teilnehmers herauszufinden, und*
- *die Möglichkeit, die Daten der Teilnehmer nach Straßen und Häusern auszuwerten und so auf die Wohnsituation zu schließen.*

Bislang war es recht unverfänglich, seine Telefonnummer in „anonymen" Kleinanzeigen anzugeben oder auf den Bierdeckel eines Verehrers zu schreiben. Nun muß man

damit rechnen, daß der Interessierte mit nicht unbedingt lauteren Absichten gleich vor der Haustür steht. Neben Privatleuten wollen auch **Behörden** die **CD-ROMs nutzen**, um die neuerdings erhöhten telefonischen Auskunftskosten zu reduzieren. Aus diesem Grund haben mehrere Verwaltungen angefragt, ob dies zulässig ist.

Die neuen Gesetze und Verordnungen im Telekommunikationsbereich (vgl. Tz. 7.3) sehen vor, daß diese Daten nur dann in elektronischen Verzeichnissen herausgegeben werden dürfen, wenn die **Betroffenen** in angemessener Weise **informiert** wurden und **nicht widersprochen** haben. Erst danach ist eine Nutzung durch Verwaltungsbehörden unbedenklich. Die Telekom hat daraufhin ihre Kunden angeschrieben und sie darauf hingewiesen, daß sie jederzeit gegen die Veröffentlichung ihrer Daten Widerspruch einlegen können, der dann ab der nächsten Version der Disk berücksichtigt wird.

Für einige private Herausgeber scheint jedoch gerade die Unrechtmäßigkeit ihrer CD-ROM das beste Werbeargument zu sein. Bislang ist z.B. der Vertrieb jeder neuen Version der „D-Info" kurz nach ihrem Erscheinen von den Gerichten untersagt worden. Zu dem Zeitpunkt waren aber bereits jeweils einige hunderttausend Exemplare im Handel, so daß ein Auslieferungsstopp wirkungslos war.

Betroffene haben zwar das Recht zu verlangen, daß ihre Daten zumindest in künftigen Versionen der CD-ROM weggelassen werden. Solchen Löschungsanträgen ist man jedoch nicht nachgekommen, vielmehr entzieht man sich durch einen Trick jeglicher Verpflichtung: Für jede Version wird ein eigenständiger Verlag gegründet. Alle Ansprüche gegen den einen Verlag müssen jeweils neu gegen den nächsten Verlag gestellt werden. Dann aber ist die „Silberscheibe" bereits im Handel. Da staunt der Bürger, und auch der Richter wundert sich: Es fehlt die wirksame rechtliche Handhabe, den Vertrieb der CD-ROM zu unterbinden. So bleibt nur noch die Möglichkeit für jeden, seinen Teilnehmereintrag im Telefonbuch auf das Nötigste zu beschränken.

Was ist zu tun?

Der Bürger sollte sich genau überlegen, ob und mit welchen Angaben er in welchen Telefon- und Adreß-CD-ROM-Verzeichnissen stehen möchte.

7.5 Datenschutz durch Technik - ein Rückblick auf die Sommerakademie 1996

Neben Risiken bietet die Technik in zunehmendem Maße auch Problemlösungen. Datenschutz durch Technik eröffnet neue Chancen für effektiveren Datenschutz.

Die wachsende Abhängigkeit von schnell verfügbaren und korrekten Informationen aus den Computern birgt große Gefahren, denen es mit rechtlichen, organisatorischen und technischen Maßnahmen zu begegnen gilt. **Neue Technologien** bieten dabei häufig die **Chance**, Datenschutz und Datensicherheit besser zu realisieren, als dies in herkömmlichen Verfahren möglich war. Um eine datenschutzgerechte Technikgestaltung zu erreichen, müssen allerdings folgende Grundsätze beachtet werden:

- **Datensparsame Technik**: Nur die wirklich erforderlichen Daten dürfen überhaupt erhoben und gespeichert werden, sie müssen sofort wieder gelöscht werden, sobald sie nicht mehr erforderlich sind. Oft können auch organisatorische Regeln umfangreiche Datensammlungen vermeiden, z.B. bei Abrechnungssystemen durch Pauschaltarife oder vorausbezahlte anonyme Chipkarten (Prepaid-Chipkarten). Wo die Speicherung individueller Daten unverzichtbar ist, reichen manchmal Pseudonyme aus, also zusätzliche Identitäten, die der Benutzer selbst wählt. Wird diese Zuordnung bei vertrauenswürdigen Stellen gespeichert, darf sie nur unter bestimmten strengen Voraussetzungen aufgedeckt werden, z.B. auf richterlichen Beschluß bei Verdacht von Straftaten.

- **Zugriffsschutz**: Für die gespeicherten Daten muß eine enge Zweckbindung gewährleistet sein, Unbefugte dürfen die Daten weder zur Kenntnis nehmen noch verändern, fälschen oder zerstören können. Ein Zugriffsschutz läßt sich mit Paßworten, Vergabe von maßgeschneiderten Zugriffsrechten und einer wirksamen Verschlüsselung (vgl. Tz. 7.6) erreichen. Einen Schutz gegen unbemerkte Veränderung bietet die digitale Signatur (vgl. Tz. 7.7). Flankierende Maßnahmen sind das regelmäßige Anfertigen von Sicherungskopien und eine umfassende Zugriffsprotokollierung, die nicht manipulierbar sein darf.

- **Kontrolle durch den Betroffenen selbst**: Wer seine Daten preisgibt, muß die Chance haben, sich über deren weitere Verwendung zu informieren. Eine effektive Verfügungs- und Kontrollgewalt läßt sich z.B. dadurch erreichen, daß die Daten beim Betroffenen selbst gespeichert werden (z.B. auf einer Chipkarte).

- **Transparenz**: Die technischen Systeme müssen so transparent aufgebaut sein, daß der Anwender sowohl erkennen als auch steuern kann, wo welche seiner Daten gespeichert und übertragen werden. Die

Sicherheitsrisiken für die Daten müssen vom Benutzer abschätzbar sein.

- **Nachprüfbarkeit**: Die Kosten für schnelle Verarbeitung und großen Speicherplatz sind inzwischen so gering, daß durch entsprechend gesicherte Protokollierungen alle wesentlichen Verarbeitungsschritte auf Dauer transparent gemacht werden können (z.B. umfassende Archivierung auf Bildplatten).

Eine **grundrechtsfreundliche Technikgestaltung** bedingt nicht zwangsläufig tiefgreifende technisch-wissenschaftliche Erkenntnisse. Oft reichen pfiffige Ideen aus, um einen wirksamen Datenschutz und eine angemessene Datensicherheit zu unterstützen.

- Verschlüsselungssysteme für elektronisch gespeicherte Daten sind fast schon ein alter Hut. Inzwischen arbeiten auch Sprach- und Faxverschlüsselungsgeräte ohne merkbare Verzögerung beim Telefonieren.

- Ein anderes System basiert auf einer Identifikationskarte, die der Benutzer bei sich trägt. Entfernt er sich von seinem Rechner, verdunkelt sich der Bildschirm, und der Computer wird „verriegelt", so daß weder Eingaben noch ein Neustart möglich sind. Mit der Rückkehr des Benutzers wird der Rechner wieder freigeschaltet.

- Videokonferenzsysteme werden zwar noch nicht im großen Stil eingesetzt, doch es gibt bereits eine Software, um geheime Informationen unbemerkbar von abhörenden Dritten in die Bewegtbildübertragung einzubetten.

- Datenträger, die außer Haus vernichtet werden sollen, lassen sich ohne die Möglichkeit eines unberechtigten Zugriffs zu einem Kunststoffkuchen einschmelzen, indem ein besonderes Verschlußsystem mit höherem Schmelzpunkt verwendet wird.

Leider sind Maßnahmen zu Datenschutz und Datensicherheit beim Gestalten und Betreiben von technischen Systemen noch nicht selbstverständlich. Wenn jedoch neue Technologien nicht bereits unter Sicherheitsaspekten entwickelt, lassen sich zusätzliche technische Maßnahmen zum Schutz des einzelnen meist nur schwer nachträglich aufsetzen. Viele Unternehmen haben deshalb inzwischen erkannt, daß bei den Verbrauchern ein realer Bedarf an datenschutzgerechter Technikgestaltung besteht und betrachten einen eingebauten Datenschutz als **Marketing-Vorteil**.

Einige dieser Produkte waren bei der Sommerakademie '96 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN in Kiel zu sehen. Für die Akzeptanz der Technik des Informationszeitalters wird es entscheidend sein, ob Datenschutz, Datensicherheit und Revisionsfähigkeit von Anfang an als „Feature" integriert sind.

Was ist zu tun?
Die Hersteller sollten derartige Techniken anbieten. Die Verwaltung und die Verbraucher sollten dies verlangen.

7.6 Krypto kontrovers

Kryptographie, die Lehre von der Verschlüsselung, ist schon einige tausend Jahre alt. In den letzen Jahren ist diese Wissenschaft aus der Geheimdienstecke herausgekommen, so daß viele Verschlüsselungsverfahren offengelegt und von Experten und anderen Interessierten auf Stärken und Schwächen hin untersucht werden. Das Recht der Bürger, schützenswerte Daten zu verschlüsseln, sollte nicht eingeschränkt werden.

Heute ist jeder Home-PC in der Lage, **schnell** und **wirksam** zu **verschlüsseln**. Gerade im Hinblick auf die Informationsgesellschaft, zu der wir uns entwickeln, gewinnt dieser Schutz der Informationen vor unbefugten Zugriffen an Bedeutung. Mit wirksamen Verschlüsselungsverfahren kann man erreichen, daß die chiffrierten Daten nicht von Außenstehenden verstanden werden. Außerdem können kryptographische Verfahren zum „elektronischen Unterschreiben" (vgl. Tz. 7.7) eingesetzt werden, um die Daten vor einer unerkannten Veränderung zu schützen.

Stichwort: Verschlüsselung
Umwandlung eines Klartextes in einen chiffrierten Text, der nur von Eingeweihten verstanden werden soll. Zum Beispiel könnte „8iUxt#Ä@Cn" im Klartext „Datenschutz" bedeuten. Wirksame Verschlüsselungsverfahren schützen auch, wenn Angreifer das Verfahren, nicht aber den zwischen den Teilnehmern vereinbarten Schlüssel kennen. Bekannte Programme zur Verschlüsselung von elektronischer Post sind PGP (Pretty Good Privacy) und PEM (Privacy Enhanced Mail).

Eine absolute Sicherheit im mathematischen Sinn läßt sich zwar auch durch Verschlüsselung zumeist nicht realisieren, jedoch kann die **faktische Sicherheit** sehr hoch eingeschätzt werden, da ein Codebrecher selbst mit moderner Hardware durchschnittlich einige tausend Jahre bräuchte, um den Klartext herauszufinden. Da die Rechnerkapazitäten immer größer werden und Entwicklungen in der Mathematik, die die Grundlage der meisten Verschlüsselungsverfahren bildet, ständig fortschreiten, muß die Sicherheit der eingesetzten Verfahren und der verwendeten Schlüssellängen trotzdem immer wieder neu bewertet werden.

Deswegen ist eine offene Diskussion über die Verfahren und Angriffsmöglichkeiten so wichtig.

Der Alltagseinsatz von Verschlüsselungsverfahren bringt also eine so große Sicherheit, daß sich die Sicherheitsbehörden bereits Sorgen machen, daß die staatlichen Überwachungsmaßnahmen künftig ins Leere laufen. Daher prüft die Bundesregierung zur Zeit, ob Regelungen notwendig und sinnvoll sind, die bei Vorliegen einer rechtmäßigen Überwachungsanordnung im Falle einer verschlüsselten Kommunikation eine Entschlüsselung ermöglichen. Drei Arten von **Krypto-Reglementierungen** wären denkbar:

- Die Verschlüsselung wird generell verboten. Staatliche Ausnahmegenehmigungen werden nur in besonderen Fällen erteilt.

- Es werden nur Verschlüsselungsverfahren mit Soll-Bruchstellen, die den Überwachungsbehörden bekannt sind, zugelassen.

- Die Verschlüsselung ist nur zulässig, wenn die verwendeten Algorithmenschlüssel ganz oder teilweise an einer Stelle hinterlegt sind, wo sie im Zugriff der Überwachungsbehörden sind.

Verschlüsselt man nicht oder nur ungenügend, gibt es keine sichere Kommunikation in offenen Netzen. Schon im wirtschaftlichen Interesse wären die ersten beiden genannten Möglichkeiten einer Kryptoregulierung nicht tragbar, denn Kriminelle oder ausländische Geheimdienste könnten dann mit wenig Aufwand die elektronischen Informationen mitlesen. Zur Realisierung der dritten Möglichkeit wäre eine sichere und verläßliche Infrastruktur der Schlüsselhinterlegungsstellen notwendig.

Jede Form der Krypto-Reglementierung ließe sich aber **leicht umgehen**. Zum Beispiel könnten die Kommunikationspartner einen eigenen Code absprechen, so daß womöglich der Nachricht nicht anzusehen ist, daß sie versteckte Informationen beinhaltet (**Steganographie**). Außerdem könnte man Daten, die mit einem zugelassenen Verschlüsselungsverfahren chiffriert werden, vorher mit einem anderen Verfahren „vor-verschlüsseln". Erst während einer Überwachungsmaßnahme mit Entschlüsselung würde festgestellt werden, daß hier eine zusätzliche Sicherung eingebaut ist.

Der erhoffte Nutzen bei der Bekämpfung der organisierten Kriminalität und der Verhinderung von Straftaten würde sich daher wohl kaum einstellen. Statt dessen brächte eine Reglementierung mit sich, daß erhebliche **Kosten zur Überwachung** der Regelungen und zum Aufbau einer Kontrollinfrastruktur entstünden und die Daten der Bürger wegen des mangelhaften Schutzes vermehrt kriminellen Angriffen ausgesetzt wären. Die Sicherheit der Informationsgesellschaft hängt in großem Ausmaße von kryptographischen Verfahren ab. Daher treten wir dafür ein, daß die Bürger auch weiterhin ohne Einschränkung beliebige

Verschlüsselungsverfahren benutzen dürfen, so daß der Schutz ihrer Daten technisch auf hohem Niveau unterstützt wird.

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

7.7 Elektronisch unterschreiben

Die Abwicklung von rechtlich und wirtschaftlich relevanten Transaktionen über Netze setzt die Einführung digitaler Signaturen voraus. Ein Gesetzentwurf der Bundesregierung soll die gesetzlichen Grundlagen schaffen.

Wie der Handschlag, mit dem früher Verträge besiegelt wurden, ist heutzutage häufig die **Unterschrift** Zeichen einer Willenserklärung. Es ist wichtig, daß sie individuelle Züge trägt, um eine möglichst eindeutige Zuordnung zum Unterzeichner zu bekommen. Grundsätzlich muß die Unterschrift eigenhändig vollzogen werden, d.h. eine Vervielfältigung z.B. durch Telefax reicht in der Regel nicht aus.

Immer mehr Dokumente werden über Datennetze geschickt. Bis jetzt fehlt übertragenen Informationen die eindeutige Beweisbarkeit und Zurechenbarkeit, d.h. wirklich wichtige Rechtsgeschäfte lassen sich heute auf diese Weise praktisch nicht abwickeln. Die elektronische Kommunikation ist aber ein fundamentaler Baustein der Informationsgesellschaft. Technische Möglichkeiten für eine Art elektronischer Unterschrift, die **digitale Signatur**, gibt es schon lange. Nur fehlten bislang die Gesetze für eine allgemeine Anerkennung einer digitalen Signatur. Wegen der unabdingbaren Fälschungssicherheit müssen nämlich hohe Maßstäbe an die technischen und organisatorischen Voraussetzungen gelegt werden.

Stichwort: Digitale Signatur
Eine digitale Signatur dient als Siegel zu digitalen Daten. Sie wird mit Hilfe eines kryptographischen Verfahrens und eines eindeutigen „privaten" Schlüssels erzeugt. Mit dem zugehörigen „öffentlichen" Schlüssel kann die Signatur jederzeit überprüft und damit der Unterzeichner und die Unverfälschtheit der Daten festgestellt werden. Im Gegensatz zur handgeschriebenen Unterschrift ist die digitale Signatur sehr schwer zu fälschen.

Ab **1997** soll es losgehen: Man geht an seinen PC, wählt das zu signierende elektronische Dokument aus, steckt seine Chipkarte mit dem privaten Schlüssel und der Signiertechnik in das Lesegerät am Computer, identifiziert sich über eine Nummer (PIN) und gibt den Befehl zum Signieren. Prompt wird das Dokument mit der digitalen Signatur des Benutzers versehen.

Nach dem Entwurf des **Signaturgesetzes** (SigG) soll jeder seinen Signaturschlüssel bei einer der zugelassenen Zertifizierungsstellen bekommen, die weitgehende Sicherheitsanforderungen erfüllen müssen. Niemand soll den entscheidenden privaten Schlüssel auslesen können. Deswegen dürfen nach dem Entwurf diese privaten Schlüssel nicht bei den Zertifizierungsstellen gespeichert werden, die solche Schlüsselpaare mit Hilfe eines Rauschgenerators erzeugen und sofort auf der Chipkarte ablegen. Dasselbe gilt für Identifikationsdaten wie die PIN, mit der der Benutzer seine Chipkarte zum Signieren freischaltet.

Es ist zu begrüßen, daß man nicht nur mit seinem Namen, sondern auch mit Pseudonymen unterschreiben können soll. Gerade in Datennetzen lassen sich aus mit dem Namen signierten Daten Persönlichkeitsprofile (z.B. bezüglich des Kaufverhaltens von Personen) erstellen. **Pseudonyme** erschweren die Zuordnung signierter Daten zu einer Person.

Im Gesetzentwurf werden die beteiligten Stellen nicht zur Offenlegung ihrer Technik verpflichtet. Ohne Vertrauen zu den Zertifizierungsstellen und der Technik wird sich aber die digitale Signatur nicht durchsetzen können. Vertrauen bildet sich nur, wenn mit **offenen Karten** gespielt wird. Daher fordern wir, daß sich jeder bei Bedarf Einblick in die verwendeten Verfahren und die Funktionsweise aller Komponenten verschaffen kann, die zur digitalen Signatur gehören. Auch wenn es viele womöglich gar nicht so genau wissen wollen, ist es doch wichtig, daß die Interessierten offen diskutieren können. Zudem wird damit die Gefahr von unentdeckten „Hintertüren" reduziert.

Was ist zu tun?
Der Gesetzgeber sollte die Vorschläge des Datenschutzes im Signaturgesetz berücksichtigen.

7.8 Schleswig-Holstein-Netz

Eine Kontrolle des Schleswig-Holstein-Netzes förderte konzeptionelle Sicherheitsmängel zutage. Bislang fehlt ein Sicherheitskonzept.

Das Schleswig-Holstein-Netz ist ein Angebot der Datenzentrale Schleswig-Holstein, beliebige Daten über angemietete Leitungen der Telekom und eigene Vermittlungsrechner zu übertragen. Dabei sind die meisten Vermittlungsrechner in Räumlichkeiten außerhalb der Datenzentrale untergebracht. Unter den etwa hundert Nutzern des Schleswig-Holstein-Netzes befinden sich auch die Staatsanwaltschaften, die **sensible Daten** untereinander austauschen. Bereits im 18. Tätigkeitsbericht (vgl. Tz. 7.3) hatten wir für das Schleswig-Holstein-Netz ein Sicherheitskonzept angemahnt. Eine Prüfung sollte zeigen, was sich seitdem getan hat.

Zu Beginn der Prüfung existierten **keine prüffähigen Unterlagen**. Außer der pauschalen Aussage, die Datenzentrale gewähre im Rahmen der betrieblichen und technischen Möglichkeiten ein Maximum an Datensicherheit, gab es keine Informationen. Allerdings waren wir durch ein Schreiben der Datenzentrale alarmiert, daß Knotenrechner, Router und Gateways teilweise in unabgesicherten Räumen stehen. Daher konnte nicht ausgeschlossen werden, daß auch Unbefugte die im Klartext übertragenen Daten lesen bzw. entwenden konnten.

Im Verlauf der Prüfung hat die Datenzentrale mit den **Nachbesserungen** begonnen. So wurden Entwürfe für ein Sicherheitskonzept, für eine Dienstanweisung für den Netzbetrieb, für einen Mietvertrag mit den Behörden, die die Vermittlungsrechner beherbergen, und schließlich für einen neuen Nutzungsvertrag vorgelegt. Doch auch bei Abschluß der Prüfung wiesen insbesondere der Nutzungsvertrag und das Sicherheitskonzept noch erhebliche Mängel auf. Eine Risikoanalyse, die immer dann erstellt werden muß, wenn personenbezogene Daten betroffen sind, die einem besonderen Amts- oder Berufsgeheimnis unterliegen, fehlt bislang ganz.

Gerade für ein Angebot wie das Schleswig-Holstein-Netz, das vielseitig genutzt und in Kombination mit anderen Verfahren zum Einsatz kommen kann, sind ein **hohes Datensicherheitsniveau** und eine umfassende Dokumentation **unabdingbar**. In den Fällen, in denen die Kunden selbst öffentliche Stellen sind, haben sie nicht nur das Recht, sondern vielmehr die Pflicht, vor der Nutzung die Maßnahmen für Datenschutz und Datensicherheit zu hinterfragen und bei einem unbefriedigenden Ergebnis von einer Nutzung abzusehen.

Die Datenzentrale konnte bis zum Redaktionsschluß dieses Berichts noch keine abschließende Stellungnahme abgeben. Es wurde lediglich eine vielversprechende Grundlagenarbeit zu Datenschutz und Datensicherheit im Schleswig-Holstein-Netz vorgelegt, deren Ergebnisse aber noch nicht in das Sicherheitskonzept eingeflossen sind. Dieses Sicherheitskonzept soll allen Kunden zur Verfügung gestellt werden, damit sie im Rahmen ihrer eigenen Verantwortung über ggf. zusätzlich zu treffende Maßnahmen entscheiden können.

Was ist zu tun?

Die Datenzentrale Schleswig-Holstein muß die für das Schleswig-Holstein-Netz getroffenen Datensicherheitsmaßnahmen dokumentieren und nachbessern. Die Kunden sollten darauf achten, daß in ihren Nutzungsverträgen das erforderliche Sicherheitsniveau festgeschrieben wird.

7.9 IKONET

Eine Kontrolle des Kommunikationsnetzes IKONET im Innenministerium zeigte Sicherheitsmängel. Sensible Daten sind bei Übermittlungen weitgehend ungeschützt, der Virenschutz ist nicht ausreichend.

Landtag, Staatskanzlei und die Ministerien sind in Schleswig-Holstein über das sogenannte **IKONET** vernetzt, das vom Innenministerium betreut wird. Das Rechnernetz bietet die Möglichkeit, ein gemeinsames Ablagesystem für Dokumente zu nutzen und elektronische Nachrichten (E-Mails) zwischen den einzelnen Ressorts, aber auch mit Kommunikationspartnern außerhalb des Netzes, z.B. im Internet, auszutauschen. In einer Prüfung haben wir diesen E-Mail-Dienst unter die Lupe genommen.

Stichwort: IKONET
*IKONET steht für Informations- und **Kommunikationsnetz** und verbindet die lokalen Rechnernetze von Landtagsverwaltung, Staatskanzlei und allen Ministerien. Als ressortübergreifende Dienste werden z.B. eine gemeinsame Dokumentenablage und das E-Mail-System zur Verfügung gestellt.*

In der Regel kann eine **E-Mail** nicht direkt zugestellt werden, sondern muß über mehrere Zwischenstationen geleitet werden. Jede dieser Zwischenstationen speichert die Nachricht eine Zeitlang, bis die Verbindung zur nächsten Station aufgebaut ist, und leitet sie dann dorthin weiter. Ein Angreifer mit Zugriff auf die Zwischenstationen oder die Leitung kann E-Mails abhören, verändern, fälschen oder unterdrükken.

Stichwort: E-Mail
In Computernetzen versandte persönliche Nachrichten bezeichnet man als elektronische Post oder „Electronic Mail", kurz E-Mail. Um elektronische Nachrichten zu verschicken, benötigen Absender und Empfänger Adressen, die ähnlich der postalischen Anschrift aufgebaut sind und von den Rechnern entlang des Übertragungsweges zugeordnet werden können. Auf diese Weise lassen sich beliebige Dateien austauschen.

Im IKONET wird eine Mail-Software eingesetzt, die zwar einem internationalen Standard (X.400 in der Version von 1984) genügt, die jedoch nicht die Möglichkeit zur Verschlüsselung (vgl. Tz. 7.6) und zur digitalen Signatur (vgl. Tz. 7.7) bietet. Dies bedeutet, daß die **Nachrichten ungeschützt** über Leitungen und Zwischenstationen geleitet werden. Versendet ein Ressort personenbezogene oder andere vertrauliche Dokumente über das IKONET, kann es die Unversehrtheit und Vertraulichkeit der Informationen dann nicht mehr selbst gewährleisten, wenn die Nachrichten das Netz im eigenen Haus verlassen. Die absendende Behörde also muß die Betreiber der Zwischenstationen schriftlich beauftragen, für sie

die Nachrichten unter Gewährleistung des erforderlichen Datensicherheitsniveaus weiterzuleiten, und die Einhaltung dieser Weisungen kontrollieren (Auftragsdatenverarbeitung i.S.d. LDSG, vgl. auch Tz. 7.8).

Solche Aufträge für den Datenaustausch im IKONET liegen bislang nicht vor: Die **Ressorts** haben es versäumt, mit dem **Innenministerium** zu vereinbaren, wie mit den personenbezogenen Daten in E-Mails zu verfahren ist. Das Innenministerium seinerseits hätte ohne Weisung der Ressorts die Daten gar nicht weiterleiten dürfen. Entsprechende Regelungen sind zu treffen, wenn die Nachrichten das IKONET verlassen und von anderen Betreibern übernommen und weitergeleitet werden.

Zwar hat das Innenministerium im Rahmen der Möglichkeiten der eingesetzten Produkte bereits einige Datensicherheitsmaßnahmen ergriffen, z.B. die Zugänge zu Leitungen und Zwischenstationen gegen Angreifer von außerhalb abgeschottet. Diese Maßnahmen reichen jedoch nicht aus, wenn es um den **Transport „sensibler" Daten** geht. Bislang sind die IKONET-Teilnehmer auf die verbleibenden Risiken nicht aufmerksam gemacht worden. Der vom Innenministerium empfohlene Schalter für „Vertraulich" im Mail-Programm suggerierte fälschlicherweise sogar einen umfassenden Schutz der elektronischen Nachricht. Wir haben dies im Rahmen der Prüfung beanstandet.

Neue Risiken sind in letzter Zeit fast unbemerkt hinzugekommen: In einigen Ressorts wurden die UNIX-Rechner durch stärker **virengefährdete Windows-PCs** ersetzt, wo auch schon die ersten per E-Mail erhaltenen Makroviren (vgl. 18. TB, Tz. 6.5) zum Zuge kamen. Außerdem hat sich die Zahl potentieller Angreifer durch die Möglichkeit, E-Mails mit Internet-Teilnehmern auszutauschen, stark erhöht. Ohne Sicherheitsmaßnahmen gegen Viren und Trojanische Pferde könnte man mit wenig Aufwand eine elektronische Nachricht mit einem Virus verschicken, der bei seiner Ausführung alle sonstigen gespeicherten Daten ausliest und per E-Mail an den Angreifer sendet.

Das Innenministerium ist bislang der Ansicht, die im IKONET getroffenen Vorkehrungen seien so weitgehend, daß ein Zugriff Unbefugter auf alle vorhandenen Daten wirksam verhindert werden dürfte. Dennoch wird in der Stellungnahme betont, es bestehe jedoch selbstverständlich die Bereitschaft, Datenschutz und Datensicherheit im IKONET stets dem Stand der Technik anzugleichen, soweit es die wirtschaftlichen Randbedingungen erlaubten. So sei z.B. beabsichtigt, eine Verschlüsselung der E-Mail einzuführen. Außerdem werde die im Innenministerium bestehende Dienstanweisung zur Benutzung der E-Mail um den Punkt „Risiken" ergänzt. Weiterhin seien bereits Maßnahmen eingeleitet, um die zentrale Verwaltung des E-Mail-Dienstes in vollem Umfang in die Zuständigkeit der Datenzentrale zu überführen, die dann je nach Anforderung entsprechende Verträge mit den nutzenden Dienststellen abschließen soll.

Inzwischen wurden unsere Bedenken bezüglich der „Ahnungslosigkeit" einiger IKONET-Teilnehmer bestätigt, als eine E-Mail **aus dem Internet** in einer angebundenen Dienststelle helle Aufregung verursachte: Die Dienststellenleitung war nämlich davon ausgegangen, daß eine elektronische Kommunikation mit Teilnehmern außerhalb des IKONET nicht möglich sei.

Was ist zu tun?
Die veraltete Mail-Software sollte durch ein Produkt mit mehr Sicherheitsfunktionalität ersetzt werden. Alle Teilnehmer sollten sich über Risiken im IKONET informieren und zusätzliche Sicherheitsmaßnahmen treffen, um die elektronisch ausgetauschten Daten ausreichend zu schützen.

8. Europäische ISDN-Richtlinie

Die europäischen Mühlen mahlen langsam. Nun scheint es endlich so, als stünde die Telekommunikations-Datenschutz-Richtlinie der EU unmittelbar vor der Verabschiedung.

Schon im 17. Tätigkeitsbericht (vgl. Tz. 7.1) und im 18. Tätigkeitsbericht (vgl. Tz. 8.2) haben wir über den Stand der Arbeiten an der „Richtlinie des Europäischen Parlamentes und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in digitalen Mobilfunknetzen" berichtet. Nach unserer Auffassung muß die für 1998 vorgesehene **Liberalisierung des Telekommunikationsmarktes** in der Europäischen Union unbedingt von einer datenschutzrechtlichen Regelung begleitet werden, die auf die besonderen Gefahren der Datenverarbeitung im Zusammenhang mit Telekommunikationsvorgängen eingeht.

Die Vorarbeiten der EU an einer solchen Richtlinie reichen bis in das Jahr 1990 zurück. In der jetzt vorliegenden Fassung (vom 12.09.1996) trägt der Entwurf den wesentlichen Gesichtspunkten des Datenschutzes Rechnung. Die Mitgliedstaaten werden verpflichtet, Regelungen über die **Vertraulichkeit der Telekommunikation** zu treffen.

- Daten über einzelne Telekommunikationsverbindungen dürfen - soweit keine weitergehende Einwilligung vorliegt - nur zur Gebührenabrechnung verwendet werden.

- Werden Daten dafür nicht gebraucht, sind sie nach Beendigung der Verbindung zu löschen.

Diese Forderungen werden in wesentlichen Teilen bereits durch die deutschen Regelungen im Telekommunikationsgesetz (vgl. Tz. 7.3.1) und in der Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) (vgl. Tz. 7.3.2) erfüllt.

Allerdings ergibt sich auch für das deutsche Recht ein Änderungsbedarf. So verlangt die Richtlinie, daß Anrufe zu Zwecken des **Direktmarketings** nicht gegen den Willen der Angerufenen erfolgen dürfen. Bei Verwendung von Automaten als Anrufern ist sogar die vorherige Einwilligung der Teilnehmer erforderlich. Direktmarketinganrufe haben sich insbesondere in den USA als eine wahre Plage des Telefonverkehrs erwiesen. Es ist nicht ungewöhnlich, dort mit den sogenannten Junk-Calls durchgehend von 17.00 Uhr bis 22.00 Uhr belästigt zu werden.

Daher ist es sinnvoll, einer solchen Praxis europaweit einen Riegel vorzuschieben. Den Mitgliedstaaten steht jedoch ein gewisser Spielraum bei der Umsetzung in innerstaatliches Recht zu.

Was ist zu tun?

Die Landesregierung sollte im Rahmen ihrer Einflußmöglichkeiten darauf hinwirken, daß die ISDN-Richtlinie in der vorliegenden Form in Kraft tritt und nicht im weiteren Verfahren wieder verwässert wird.

9. Was es sonst noch zu berichten gibt

9.1 Darf ein Gemeindevertreter Personalakten einsehen?

Ein Gemeindevertreter wollte sich über den Inhalt des Arbeitsvertrages unterrichten, den die Amtsverwaltung mit dem Hausmeister des kommunalen Gemeinschaftshauses abgeschlossen hatte. Er erbat zu diesem Zweck eine Kopie des Vertrages. Dies wurde ihm unter Hinweis auf „den Datenschutz" verweigert. Zu recht, denn nach der Gemeindeordnung ist zwar einzelnen Gemeindevertretern auf Verlangen Auskunft zu erteilen und Akteneinsicht zu gewähren, bei Personalakten gilt das allerdings nur für die Mitglieder des Hauptausschusses oder eines Personalausschusses.

9.2 Förmliche Anhörverfahren: Einwender müssen einander nicht alle kennen

Ein Kreis lud als untere Wasserbehörde im Rahmen eines wasserrechtlichen Genehmigungsverfahrens alle Einwender zu einem Erörterungstermin ein. Dem Einladungsschreiben war eine Namensliste aller Einwender beigefügt. Die Einlassung der Wasserbehörde, dies erscheine datenschutzrechtlich unbedenklich, da doch jeder Beteiligte im Rahmen seines Akteneinsichtsrechts die Daten der anderen ohnehin zur Kenntnis hätte nehmen können, war nicht stichhaltig, denn Daten einzelner Einwender müssen nicht zwangsläufig im Rahmen von Auskünften auch allen anderen Beteiligten offenbart werden. Da also kein Einwender einen Anspruch hat, die Identität der anderen Einwender zu kennen, hatte die Behörde auch nicht das Recht, sie publik zu machen.

9.3 Umgang mit Stundungsanträgen

Vermehrt erreichten uns Eingaben und Beratungsersuchen im Zusammenhang mit Stundungsanträgen. In einem Fall rieten wir einer Gemeinde, den Namen von Antragstellern nicht automatisch zu den Sitzungsunterlagen zu geben, sondern nur dann, wenn dies zur Entscheidung über den Antrag notwendig ist. In einem anderen Fall ergab unsere Überprüfung, daß in dem Stundungsantrag weit mehr Daten abgefragt wurden als für das Stundungsverfahren notwendig. Einige Angaben, wie z.B. zu den wirtschaftlichen Verhältnissen der Angehörigen, wurden daraufhin gestrichen.

9.4 Wenn es die Gemeinde zu genau wissen will

Mehrere Gemeinden eines Amtes hatten per Haushaltsfragebogen mit detaillierten Angaben über die persönlichen Verhältnisse der Familien Grundlagendaten für die künftige Ortsentwicklung ermitteln wollen. Sie

wurden zwar ohne Namensangaben erhoben, insbesondere bei den kleineren Gemeinden war jedoch ein Rückschluß auf bestimmte Haushalte möglich. Solche Haushaltsbefragungen müssen wie Statistiken behandelt werden. Sind die Fragen so detailliert, daß auch ohne direkte Angaben zur Person eine Personenbeziehbarkeit herstellbar ist, so bedarf es für die Erhebung einer Rechtsgrundlage in einer Satzung. Im konkreten Fall haben wir Hinweise gegeben, wie die schon begonnene Befragung zu Ende gebracht und die Auswertung so durchgeführt werden konnte, daß die datenschutzrechtlichen Belange der Bürger gewahrt wurden.

9.5 Statistikgeheimnis verletzt

Die Datenübermittlungen der Gemeinden zur Erstellung der Wanderungsstatistik wurden nach einem Runderlaß des Innenministers aus dem Jahre 1953 bis vor kurzem über die jeweiligen Kreisverwaltungen an das Statistische Landesamt zugesandt, obwohl die Meldedatenübermittlungsverordnung von 1985 die unmittelbare Datenübermittlung von den Meldebehörden an das Statistische Landesamt ausdrücklich vorschreibt. Auf unsere Kritik hin hat das Innenministerium den alten Erlaß inzwischen aufgehoben.

9.6 Darf man seine eigene Zeugenaussage nicht einsehen?

Es kommt immer wieder vor, daß berechtigte Informationsersuchen der Bürger unter Hinweis auf angebliche Belange des Datenschutzes verweigert werden. Einer Zeugin sollte sogar ihre eigene Aussage unter Berufung auf „Datenschutz" vorenthalten werden. Das Datenschutzrecht stand einer Aushändigung der Kopie des Protokolls jedoch keinesfalls entgegen, weil es nur Angaben enthielt, die die Petentin selbst gemacht hatte. Mit der Kopie des Protokolls gelangte sie nicht in den Besitz neuer Informationen. Ein entsprechender Hinweis an die zuständige Stelle führte dazu, daß die Petentin eine Kopie ihres Aussageprotokolls ausgehändigt bekam.

9.7 Was man mit der Krankenversichertenkarte alles machen könnte

Im Zusammenhang mit der Nutzung der Krankenversichertenkarte (Chipkarte) haben die Versicherten nach wie vor die Sorge, daß es zu einer zweckfremden Nutzung kommen könnte. Dies scheint auch nicht unbegründet zu sein. So erreichte uns beispielsweise die Anfrage, ob die Verwendung der Krankenversichertenkarte auch für Zwecke der Zeiterfassung in einem Betrieb zulässig sei. Der Gesetzgeber hat die Nutzung der Krankenversichertenkarte im Sozialgesetzbuch V eindeutig geregelt. Damit hat er unmißverständlich klargestellt, daß die Verwendung der Krankenversichertenkarte ausschließlich für diesen Zweck zulässig ist. Daraus ergibt sich ein Verbot, die Krankenversichertenkarte zur Zeiterfassung von Arbeitnehmern innerhalb eines Betriebes zu verwenden.

9.8 Zuviel Transparenz bei Beurteilungen

Eine Landesbehörde gab im Rahmen der Zusammenarbeit nach dem Mitbestimmungsgesetz dem für sie zuständigen Bezirkspersonalrat statistische Auswertungen einer Beurteilungsaktion an die Hand. Sie umfaßten alle Beurteilungen auch der nachgeordneten Dienststellen und ließen in einigen Einzelfällen Rückschlüsse auf einzelne Mitarbeiter zu. Der Bezirkspersonalrat gab die genannten Informationen an alle örtlichen Personalräte seines Bezirkes und an eine nicht dem Personalrat angehörende Person weiter. Einer dieser örtlichen Personalräte leitete seinerseits die Unterlagen den Erst- und Zweitbeurteilern seiner Dienststelle zu. Nachdem ein Betroffener uns eingeschaltet hatte, haben wir diese Verfahrensweise beanstandet.

9.9 Fahndung nach Kurgästen

Eine Kurverwaltung hatte auf dem Parkplatz einer Einwohnerin erheblich mehr parkende ortsfremde Autos festgestellt, als die abgeführte Kurtaxe erwarten ließ. Sie zeigte die Vermieterin kurzerhand wegen Ordnungswidrigkeit an. Die Bußgeldstelle des Kreises schaltete die örtliche Polizeistation ein, die nach einer Halterfeststellung die „Kurgäste“ als Zeugen vernahm. Dies empfand die Petentin als äußerst peinlich.

Wir haben wegen Verstoßes gegen das Landesdatenschutzgesetz eine Beanstandung ausgesprochen. Hier hätte die Petentin über die Erhebung der Kraftfahrzeugdaten auf ihrem Grundstück und deren beabsichtigte Weiterverarbeitung aufgeklärt werden können, ohne daß der Ermittlungserfolg gefährdet worden wäre. Sie hätte dann unter Umständen selbst zur Sachverhaltsaufklärung beitragen können, so daß sich die unangenehmen Zeugenvernehmungen womöglich erübrigt hätten.

9.10 Wenn der Amtsvorsteher mit dem Schulverbandsvorsteher ...

Ein Amtsvorsteher war zugleich stellvertretender Schulverbandsvorsteher und hielt die Tatsache des Wohnsitzwechsels „seines“ Schulleiters für wichtig genug, um den Schulverbandsvorsteher und die Bürgermeister der verbandsangehörigen Gemeinden zu unterrichten. Der Schulleiter wurde daraufhin auf diesen Wohnsitzwechsel angesprochen, was ihm offensichtlich unangenehm war. Von uns auf den datenschutzrechtlichen Verstoß gegen melderechtliche Vorschriften hingewiesen, hat sich der Amtsvorsteher schriftlich bei dem betroffenen Schulleiter entschuldigt.

9.11 Verkehrssünder werden nicht richtig aufgeklärt

Die Bußgeldstellen größerer Städte ahnden Straßenverkehrsverstöße mit Verwarnungs- und Bußgeldern. Im Rahmen eines bundesweit eingesetzten EDV-Verfahrens wird über das festgestellte Kraftfahrzeugkennzeichen durch Fernabfrage aus dem zentralen Kraftfahrzeugregister in Flensburg der Halter des Fahrzeugs ermittelt. Dies geschieht zunächst ohne seine Kenntnis. Wir haben in Prüfungen festgestellt, daß die vom LDSG geforderte nachträgliche Information der Betroffenen über Inhalt, Zweck und Rechtsgrundlage der Datenerhebung in dem eingesetzten Verfahren nicht ausreichend erfolgt. Es muß deshalb an die bestehende Rechtsgrundlage angepaßt werden. Das Verkehrsministerium hat zugesagt, entsprechende Initiativen zu ergreifen.

9.12 Ein Griff - und das Sozialgeheimnis ist dahin

Ein anonymer Besucher hatte es eilig und übergab uns ein großes Kuvert ohne Absender. Der Inhalt war brisant. Es fanden sich

- die Kopie einer Arbeitsunfähigkeitsbescheinigung,
- ein Nachweis über die Leistung gemeinnütziger Arbeit,
- die Mitteilung einer Krankenkasse über Leistungen der Pflegestufe 3,
- die Kopie eines Lohnstreifens und
- die Kopie einer Bescheinigung über Nebenverdienste.

In einem Begleitbrief teilte der Unbekannte mit, die Unterlagen habe er einem Briefkasten des Sozialamtes der Stadt Kiel mühelos von außen entnehmen können. Bisherige Beschwerden bei den Verantwortlichen hätten nicht gefruchtet. Eine kurzfristig anberaumte Inaugenscheinnahme bestätigte den Sachverhalt. Auch unsere Prüfer konnten sich in dem Briefkasten „bedienen“. Uns wurde eine umgehende bauliche Veränderung zugesagt und versichert, daß der Briefkasten bis dahin in kurzen Abständen geleert werde. Als wir bei einer Nachkontrolle feststellen mußten, daß der alte Briefkasten noch da war und offensichtlich nicht rechtzeitig geleert worden war, war es wieder möglich, Briefe zu entnehmen. Auf unsere Beanstandung hin wurde der Mangel jetzt beseitigt.

9.13 Öffentliche Informationen über nichtöffentliche Verfahren?

Warum muß bei Verfahren zur Abgabe der eidesstattlichen Versicherung der Name des Schuldners öffentlich in den Gerichten ausgehängt werden, wenn das Verfahren selbst gar nicht öffentlich ist, fragte eine Petentin. Auch nach unserer Auffassung besteht dazu keine Notwendigkeit. Da wir gegenüber den Gerichten keine Kontrollbefugnis haben, können wir nur auf diesem Weg auf das Problem aufmerksam machen und die Gerichte ermuntern, in diesen Verfahren auf den öffentlichen Aushang der Terminsrolle künftig zu verzichten.

9.14 Was fehlt noch? Jubiläumsdaten!

Sensibel zeigte sich der Personalrat einer kommunalen Dienststelle. Die Mitarbeiter wurden von der Verwaltung nämlich aufgefordert, sich in eine Liste einzutragen, wenn sie eine vorgesehene behördeninterne Veröffentlichung ihrer Geburts- und Jubiläumsdaten nicht wünschten. Der Personalrat erhob gegen diese „Negativabfrage" Bedenken. Wir sind der Meinung, der persönliche Glückwunsch im Kreis der Kollegen sei traditioneller Bestandteil des Berufslebens. Eine ausdrückliche Einwilligung der Betroffenen halten wir nicht für notwendig, sofern wenigstens eine Widerspruchsmöglichkeit besteht.

10. Rückblick

10.1 Sozialministerium entscheidet: Versorgungsämter folgen nicht den Vorschlägen des Datenschutzbeauftragten

Aufgrund einer Prüfungsmaßnahme in einem Versorgungsamt im Jahre 1995 waren von uns drei strittige Punkte zunächst an das Landesversorgungsamt und, nachdem auch hier keine Einigung erzielt werden konnte, an das Sozialministerium zur Entscheidung herangetragen worden (vgl. 18. TB, Tz. 6.7.4). Leider konnte sich das Ministerium nicht der von uns vertretenen Rechtsauffassung anschließen. Von „höchster Stelle" wurde entschieden,

- daß weiterhin Altakten mit medizinischen und Sozialdaten von gewerblichen Dienstleistern ohne Aufsicht durch die Behörde vernichtet werden,

- daß „externen" ärztlichen Gutachten nicht auferlegt wird, nur solche Antragsdaten in ihren Unterlagen aufzubewahren, die nach den standesrechtlichen Vorschriften zur Dokumentation ihrer ärztlichen Handlungen tatsächlich erforderlich sind und

- daß Mitarbeiter eines Versorgungsamtes nicht die Chance erhalten, die sie selbst betreffenden Anträge von einem anderen Amt als dem, bei dem sie beschäftigt sind, bearbeiten zu lassen.

Dem Datenschutzrecht entsprechen nach unserer Auffassung diese Entscheidungen nicht.

10.2 Schreibdienst im Krankenhaus

Im 18. Tätigkeitsbericht (vgl. Tz. 4.8.3) hatten wir die Vergabe von Schreibarbeiten an Externe durch ein öffentliches Krankenhaus kritisiert. Aufgrund unserer Beanstandung wurde diese Praxis eingestellt. Hiervon haben aber offenbar nicht alle Krankenhäuser Kenntnis erhalten, denn auch in diesem Jahr erreichten uns wieder Beschwerden, und wir mußten erneut tätig werden, weil Arztbriefe auf privaten PC zu Hause geschrieben werden sollten.

10.3 Asylcard - vielleicht eine Lösung, aber wo ist das Problem?

Wir berichteten verschiedentlich (vgl. 17. TB, Tz. 4.1.3.4) über Pläne der Innenminister, mit einer „Asylcard" ein umfassendes Identifikations- und Informationspapier für asylsuchende Ausländer zu schaffen und wiesen

darauf hin, daß die derzeitige Diskussion sich primär an den vorstellbaren technischen Möglichkeiten und den denkbaren Funktionen einer Chipkarte orientiert. Wir haben statt dessen eine Beschreibung der Aufgaben empfohlen, die durch eine Asylcard erfüllt werden sollen. Sie müßten Grundlage des Auftrags sein, der schließlich zu einer Machbarkeitsstudie führt. Die rechtlichen Grenzen und die Datenschutzgesichtspunkte sind schon bei der Aufgabenbeschreibung zu berücksichtigen. Nur so ist sicherzustellen, daß die „Macher" nicht der Faszination des technischen Mediums erliegen und im nachhinein Aufgaben suchen, die mit Hilfe dieser Technik gelöst werden können.

10.4 Schleswig-Holstein erhält bis auf weiteres keine eigene Rechtstatsachensammelstelle

Der Innenminister hat 1995 aufgrund unserer Anregungen zunächst die Einrichtung einer eigenen, wissenschaftlich begleiteten Rechtstatsachensammelstelle in Schleswig-Holstein zur Überprüfung polizeilicher Befugnisse in Aussicht gestellt (vgl. 18. TB, Tz. 10.1). Zwischenzeitlich hat er uns darüber in Kenntnis gesetzt, daß sich die schleswig-holsteinischen Polizeidienststellen nur an der beim Bundeskriminalamt (BKA) eingerichteten Bund-Länder-Fallsammlung beteiligen sollen. Auf die starken Zweifel an der Objektivität dieser Stelle hatten wir bereits im 18. Tätigkeitsbericht hingewiesen. Sie soll wohl vor allem der Sammlung spektakulärer Einzelfälle dienen, in denen Rechtsvorschriften hinderlich waren. Selbst unserer Anregung, bis zur Errichtung einer landeseigenen Sammelstelle die von den Dienststellen dem BKA zu meldenden Sachverhalte auch in Kopie bei einer Stelle innerhalb des Landes zu sammeln, um jedenfalls eine nachträgliche wissenschaftlich begleitete Auswertung dieses Materials zu ermöglichen, vermochte das Innenministerium nicht zu folgen. Bereits das Raster zur Erfassung der auszuwertenden Straftaten müsse nach den Gesichtspunkten der wissenschaftlichen Auswertung entwickelt werden. Dafür stünden ihm die Haushaltsmittel leider nicht zu Verfügung.

10.5 Auskunft auch bei laufenden Ermittlungsverfahren durch die speichernde Stelle

Im 18. Tätigkeitsbericht (vgl. Tz. 4.2.3) hatten wir von einem Petenten berichtet, dem die Auskunft über die Datenspeicherungen zu seiner Person durch die Polizei verweigert wurde, da das Ermittlungsverfahren gegen ihn noch nicht abgeschlossen war. Wir hatten darauf hingewiesen, daß diese Praxis nicht mit dem Auskunftsanspruch nach dem Landespolizeirecht und dem Landesdatenschutzgesetz zu vereinbaren ist. Das Innenministerium sah sich zunächst nicht zur Abhilfe in der Lage, da eine Weisung des Generalstaatsanwalts entgegenstand. In einem klärenden Gespräch mit dem Generalstaatsanwalt, dem Justizministerium und dem

Innenministerium wurde nun festgelegt, daß der Betroffene in Zukunft auch bei der Polizei Auskunft über die dort über ihn gespeicherten Informationen erhält. Zuvor soll die Polizei bei der Staatsanwaltschaft Rückfrage halten, ob eine Auskunft die Zwecke des Ermittlungsverfahrens gefährdet.

10.6 Neugestalteter Anhörungsbogen läßt Umfang des Aussageverweigerungsrechtes klar erkennen

Im 18. Tätigkeitsbericht (vgl. Tz. 4.2.2) haben wir bemängelt, daß die von der Polizei im Rahmen der Beschuldigtenvernehmung verwendeten Anhörungsbögen den Umfang des Aussageverweigerungsrechtes nicht klar wiedergaben. Das Innenministerium hat aufgrund unseres Hinweises nunmehr nach Abstimmung mit dem Justizministerium und der Generalstaatsanwaltschaft einen neugestalteten Anhörungsbogen vorgelegt. Mit diesem werden die gesetzlichen Vorgaben klar umgesetzt. Im ersten Teil werden die Pflichtangaben zur Person abgefragt, im zweiten Teil sollen weitere Angaben zur Person und den persönlichen Verhältnissen gemacht werden, wobei jedoch auf das Aussageverweigerungsrecht bezüglich dieser weitergehenden Fragen hingewiesen wird. Der dritte Teil ist den Angaben zum Tatvorwurf selbst vorbehalten. Positiv hervorzuheben ist auch, daß in dem neugestalteten Anhörungsbogen auf die routinemäßige Abfrage der Personenangaben zu den Eltern und dem Ehegatten des Beschuldigten verzichtet wird.

10.7 Noch fehlt die Verordnung im Umweltbereich

Im 18. Tätigkeitsbericht (vgl. Tz. 4.5.2) hatten wir den Erlaß der Datenschutzverordnung im Umweltrecht angemahnt. Obwohl das Umweltministerium bei der parlamentarischen Erörterung des Tätigkeitsberichts ankündigte, daß noch 1996 mit einer Verordnung zum Landeswassergesetz zu rechnen sei, liegt diese bisher noch nicht vor.

10.8 Die Kreise als Träger der Abfallentsorgung und ihre Abfallwirtschaftsgesellschaften reagieren auf unsere Kritik

Offenbar haben sich mittlerweile alle Kreise, die das Inkasso der Abfallgebühren von einer Abfallwirtschaftsgesellschaft durchführen lassen, die von uns mit dem Kreis Schleswig-Flensburg erarbeitete Musterregelung (vgl. 18. TB, Tz. 4.5.1) zu eigen gemacht und die Datenverarbeitung mit den Gesellschaften vertraglich geregelt. Eine Arbeitsgruppe aus Vertretern mehrerer Kreise, des Umweltministeriums und des Landkreistages hat ein Muster einer kompletten Abfallwirtschaftssatzung einschließlich umfangreicher Datenverarbeitungsbestimmungen entwickelt.

10.9 Verweigerung der Akteneinsicht: Das Wirtschaftsministerium greift ein

Im letzten Tätigkeitsbericht schilderten wir den Fall eines Bürgers, der Einsicht in seine Kraftfahrzeug-Zulassungsakte nehmen wollte und trotz kostspieligen Prozesses und datenschutzrechtlicher Beanstandung diese zunächst nicht erhielt (vgl. 18. TB, Tz. 4.6.4). Auch nach unserer Beanstandung und weiterem Schriftwechsel blieb der Landrat bei seiner Meinung, das rechtskräftige Urteil des Verwaltungsgerichts verbiete, dem Betroffenen Akteneinsichtsrecht zu gewähren. Erst als sich der Verkehrsminister selbst in die Angelegenheit einschaltete, wurde dem Petenten die Möglichkeit eröffnet, nun doch Einsicht in seine Zulassungsakte zu nehmen. Das hat er inzwischen getan.

10.10 Verfassungsschutzbehörde realisiert Verbesserungsvorschläge

In unserem 18. Tätigkeitsbericht (vgl. Tz. 4.3.2) haben wir über die Überschreitungen der gesetzlich festgeschriebenen Prüffristen für Datenspeicherungen durch die Verfassungschutzbehörde berichtet. Dieser Mangel ist inzwischen dadurch beseitigt worden, daß verfahrenstechnisch sichergestellt ist, daß in Frage kommende Datensätze mit einem bis zu sechsmonatigem Vorlauf listenmäßig ausgedruckt und hinsichtlich der Erforderlichkeit ihrer Weiterspeicherung geprüft werden. Weiterhin ist die Zulässigkeit von Datenspeicherungen, insbesondere zu Personen des politischen Extremismus, durch eine Arbeitsanweisung präziser festgelegt worden.

10.11 Datenaustausch zwischen Kassenärztlichen Vereinigungen und Krankenkassen

Der bereits für 1996 geplante automatisierte Datenaustausch zwischen den Kassenärztlichen Vereinigungen und den Krankenkassen ist bisher, u.a. wegen der Auseinandersetzungen über den Inhalt der Verträge noch nicht angelaufen. Die Vertreter der Zahnärzte waren gegen den Umfang des Datenaustausches Sturm gelaufen, da sie den „gläsernen Patienten“ und natürlich auch den „gläsernen Zahnarzt“ durch diesen Vertrag vorprogrammiert sahen (vgl. 18. TB, Tz. 4.8.2). Es finden zur Zeit gerichtliche Auseinandersetzungen und Verhandlungen zwischen den beteiligten Parteien statt, die im Ergebnis wohl zu einer deutlichen Verringerung des Datenprofils und damit einer Verbesserung des Datenschutzes führen werden.

10.12 Videoüberwachung im Straßenverkehr

In unserem 18. Tätigkeitsbericht (vgl. Tz. 4.2.5) haben wir dargestellt, daß bei Videoaufzeichnungen im Rahmen der Verkehrsüberwachung nicht nur Verkehrssünder, sondern auch alle gesetzestreuen Autofahrer ohne Rechtsgrundlage erfaßt werden. Die Polizei hat ihr bisheriges Verfahren insoweit modifiziert, als bei der Auswertung der Videoaufnahmen festgestellte Verstöße nunmehr aus dem Überwachungsvideoband herauskopiert, auf einem separaten Videoband archiviert und alle nicht benötigten Bildsequenzen vernichtet werden. Darin liegt eine Verbesserung, wenngleich daran festzuhalten ist, daß mit Hilfe der Videotechnik von vornherein nur solche Verkehrsteilnehmer zulässigerweise erfaßt werden dürfen, gegen die zumindest ein Anfangsverdacht erkennbar ist. Da die Polizei in anderen Bundesländern entsprechend arbeitet, scheint ein derartiges Verfahren auch mit den praktischen Bedürfnissen der Polizeibehörden vereinbar.

10.13 Aids-Hinweise in der Justizvollzugsanstalt

Im 14. Tätigkeitsbericht (vgl. Tz. 4.3.2) war unter der Überschrift „Aids-Hinweise" über die Praxis berichtet worden, auf die HIV-Infektionen von Häftlingen in der Weise aufmerksam zu machen, daß in der Gefangenenpersonalakte an vorderster Stelle der Stempel angebracht wurde: „Vorsicht! Gesundheitsakten beachten". Als sachlicher Hinweis war diese Aufschrift untauglich, denn das Recht zur Einsicht in die Gesundheitsakten hat keineswegs jeder JVA-Bedienstete, der die Gefangenenpersonalakte in die Hand bekommt, sondern nur der Arzt. Allerdings war in der JVA allgemein bekannt, daß die Bemerkung nicht etwa eine Aufforderung zur Akteneinsicht bedeutete, sondern vielmehr als Hinweis auf eine HIV-Infektion zu verstehen war. Nachdem wir diese Praxis beanstandet hatten und in verschiedenen Tätigkeitsberichten immer wieder aufgreifen mußten (vgl. 15. TB, Tz. 4.3.3; 16. TB, Tz. 4.3.2), hat das Justizministerium nunmehr durch einen Erlaß festgelegt, daß keine Hinweise auf HIV-Infektionen in der Gefangenenpersonalakte mehr eingetragen werden dürfen. Nach wie vor sind allerdings der Anstaltsarzt und der Anstaltsleiter über die HIV-Infektion eines Gefangenen unterrichtet. Dem Anstaltsleiter obliegt es zu entscheiden, welche Mitarbeiter der Anstalt und welche weiteren Personen, die mit dem Gefangenen in Kontakt kommen, von der HIV-Infektion zu unterrichten sind. Dadurch soll gewährleistet sein, daß der möglichen Gesundheitsgefährdung Dritter weiterhin vorgebeugt wird, ohne daß das informationelle Selbstbestimmungsrecht des betroffenen Gefangenen mehr als unbedingt nötig beeinträchtigt wird.

11. Beispiele, in denen die Tätigkeit des Datenschutzbeauftragten zu Verbesserungen des Grundrechtsschutzes beigetragen hat

1. *Das Kultusministerium vertrat den Standpunkt, daß Lehrer, die von ihrem Recht auf Einsicht in die Personalakte Gebrauch machen wollten, dazu extra zum Ministerium nach Kiel reisen müßten.. Nach langem Drängen ist jetzt erreicht, daß umgekehrt verfahren wird: Die Akte wird dorthin geschickt, wo der Betreffende seinen Dienst verrichtet (vgl. Tz. 4.11.2).*

2. *Noch nach Jahrzehnten konnte man in Baugenehmigungsakten Unterlagen über längst erledigte Ordnungswidrigkeitenverfahren gegen frühere Eigentümer finden. Nach unserer Beanstandung hat man begonnen, die Akten zu bereinigen und neu zu strukturieren (vgl. Tz. 4.1.1).*

3. *Einige Gemeinden waren drauf und dran, Adreßbuchverlagen die Einwohnermeldedaten zur Erfassung auf CD-ROM zu geben. Völlig neuartige und für die Bürger kaum kalkulierbare Nutzungsmöglichkeiten hätten sich daraus ergeben. Wir haben uns dafür eingesetzt, daß dies nur mit Einwilligung der betroffenen Bürger geschieht (vgl. Tz. 4.1.3).*

4. *Es bestand die Gefahr, daß die in dem automatisierten Bürokommunikationsverfahren COMPAS gespeicherten Daten (der Polizei) ein Eigenleben neben der Akte führen würden. Die Korrektur einer Zeugenaussage wäre z.B. nur im Computer, nicht aber in der Akte vermerkt worden bzw. umgekehrt. Jetzt hat der Innenminister „Gleichklang" sichergestellt. Im Zweifel gilt stets das, was in der Akte steht (vgl. Tz. 4.2.4).*

5. *Werden Führerscheine vorläufig beschlagnahmt, wird dies von der Justiz an die Fahrerlaubnisbehörden gemeldet. Wird versäumt, einen etwaigen Freispruch nachzumelden, kommt der Betroffene z.B. bei einer Fahrzeugkontrolle in die unangenehme Situation, beweisen zu müssen, daß er den Führerschein zu Recht besitzt. Der Verkehrsminister hat auf unserer Betreiben alle Behörden angewiesen, sich selbst darum zu bemühen, unvollständige Daten zu ergänzen (vgl. Tz. 4.6.4).*

6. *Wohngeldstellen verlangten von Antragstellern, sich Angaben auf den Anträgen von den Vermietern bestätigen zu lassen. Manchen ist es peinlich, wenn der Vermieter auf diesem Wege erfährt, daß Wohngeld beantragt wurde. Der Innenminister hat auf unser Drängen die Wohngeldstellen darauf hingewiesen, daß der Mieter nicht*

gezwungen werden darf, den Wohngeldantrag beim Vermieter vorzulegen, wenn er die notwendigen Informationen auch anderweitig belegen kann (vgl. Tz. 4.7.3).

7. *Auf Terminsaushängen in Gerichten konnte man nachlesen, gegen wen ein Termin zur Abgabe der eidesstattlichen Versicherung anberaumt war, obwohl das Verfahren selbst nicht öffentlich ist. Wir haben die Gerichte gebeten, in solchen Fällen auf den öffentlichen Aushang zu verzichten, damit die Betroffenen nicht ohne Not bloßgestellt werden (vgl. Tz. 5.4).*

8. *Immer mehr Behörden realisieren Sicherheitskonzepte nach unseren Vorschlägen. Dies bedeutet z.B., daß bei Diebstahl von PC aus Verwaltungsgebäuden kein Zugriff auf Daten besteht oder daß auch innerhalb der Verwaltung Datenzugriffe nur den jeweils zuständigen Bearbeitern möglich sind. Die Nutzung des in der EDV vorhandenen Sicherheitspotentials erhöht die Chance, daß Bürgerdaten nur für den gesetzlich zulässigen Zweck verwendet werden (vgl. Tz. 6.2).*

9. *Bei der Zusammenlegung der Rechenzentren der Steuerverwaltung und der Datenzentrale bestand die Gefahr, daß die sensiblen Steuerdaten den Mitarbeitern der Datenzentrale zur Kenntnis gelangten. Wir haben darauf hingewirkt, daß nicht nur die Datenbanken gegeneinander abgeschottet bleiben, sondern auch während des gesamten Verarbeitungsprozesses nur Mitarbeiter der Steuerverwaltung Zugang zu den Steuerdaten haben. So konnten eine wirtschaftlichere Aufgabenerfüllung und die Wahrung des Steuergeheimnisses miteinander in Einklang gebracht werden (vgl. Tz. 4.10.1).*

10. *Vor einigen Jahren tauchten durch einen Programmfehler in Adreßbüchern die Anschriften von Personen auf, für die wegen einer Gefahr für Leib und Leben im Melderegister Auskunftssperren vermerkt waren. Jahrelang haben wir darauf gedrängt, daß EDV-Verfahren in Zukunft besser getestet werden, bevor sie zum Einsatz kommen. Jetzt haben die kommunalen Landesverbände ein Testverfahren konzipiert, das unseren Vorstellungen entspricht. Für die Bürger in Stadt und Land heißt das konkret: Das vielzitierte „menschliche Versagen" wird im Einzelfall vielleicht auch in Zukunft zur Beeinträchtigung ihrer Rechte führen. Serienfehler aufgrund unzulänglicher Computerprogramme wird es aber seltener geben, da qualifizierte Spezialisten die Arbeit der Programmierer genauer als bisher überprüfen (vgl. Tz. 6.3).*

11. *Bislang setzt die Verwaltung im Land kaum Verschlüsselungsverfahren ein, um die Daten vor fremdem Zugriff schützen. Auf unser Drängen untersucht die Datenzentrale im Auftrag des Innenministeriums jetzt in einer Grundlagenarbeit, inwieweit kryptographische Verfahren zum Schutz der Kommunikation im Schleswig-*

Holstein-Netz und der in Datenbanken gespeicherten Informationen einsetzbar sind. Durch diese Erkenntnisse wird die Vertraulichkeit für die Daten der Bürger künftig besser gewahrt werden können (vgl. Tz. 7.8).

12. *Öffentliche Stellen mit Internet-Anschluß müssen ihr Verwaltungsnetz gegenüber Angriffen aus dem Internet schützen. Auf unsere Anregung hin wird sich die Datenzentrale mit der Frage, wie sich eine Verwaltung beim Internet-Zugang mit Hilfe von Firewall-Systemen sicher abschotten kann, in einer Grundlagenarbeit befassen. Ziel ist ein Internet-Anschluß für Verwaltungen, bei dem Unbefugte nicht auf die in den Verwaltungen gespeicherten Bürgerdaten zugreifen können (vgl. Tz. 7.8)*

13. *Fast sah es so aus, als ob Telekommunikationsanbieter verpflichtet würden, über jedes Telefonat Daten zu speichern, nur damit Sicherheitsbehörden abfragen können, wer wann mit wem telefoniert hat. Auch unser energisches Eintreten gegen diesen „Schritt in den Überwachungsstaat" hat dazu geführt, daß dieses Vorhaben nicht durchgesetzt wurde (vgl. Tz. 7.3).*

14. *Im Schleswig-Holstein-Netz der Datenzentrale, über das u.a. Daten der Staatsanwaltschaften übertragen werden, können angeschlossene Verwaltungen künftig entscheiden, welche zusätzlichen Sicherheitsmaßnahmen sie für erforderlich halten, um einen angemessenen Schutz der übertragenen Daten zu gewährleisten. Die Gefahr, daß Hacker sensible Daten über Bürger ausspähen oder manipulieren, wird minimiert (vgl. Tz. 7.8).*

15. *Bis jetzt waren sich die an die „elektronische Post der Landesregierung" angeschlossenen Verwaltungen der damit verbundenen Sicherheitsrisiken nicht hinreichend bewußt. Nach unserer Kritik werden zusätzliche Sicherheitsmaßnahmen wie Verschlüsselung und digitale Signatur eingeführt. Damit hat ein Angreifer, der die bei der Übertragung zwischengespeicherten Nachrichten mitlesen oder verändern will, kaum mehr eine Chance (vgl. Tz. 7.9).*

16. *Das schleswig-holsteinische Krebsregistergesetz hat, um möglichst alle Krebsfälle zu erfassen, eine Meldepflicht für Ärzte eingeführt. Die Erkrankten, die mit einer namentlichen Meldung nicht einverstanden sind, werden jedoch nur verschlüsselt im Krebsregister erfaßt. Wir haben zusätzlich darauf hingewirkt, daß das Register Informationen nicht an Dritte herausgeben darf, wenn im Einzelfall doch einmal das Risiko einer Identifizierungsmöglichkeit durch den Empfänger besteht. Die Gefahr, daß Daten über Krebserkrankungen in falsche Hände geraten, wurde damit verringert (vgl. Tz. 4.8.1).*

17. Bisher haben Universitätskliniken ohne Einwilligung der Betroffenen mit Patientendaten geforscht. Nunmehr werden die Patienten ausdrücklich gefragt, ob sie damit einverstanden sind (vgl. Tz. 4.8.2).

18. In einem Krankenhaus wurden die persönlichen Daten bei der Aufnahme in hörbarer Nähe zu anderen Patienten abgefragt. Aufgrund unserer Intervention wurden räumliche Umbauarbeiten vom Ministerium genehmigt. Nach ihrem Abschluß brauchen Patienten bei der Aufnahme nicht mehr intime Details in Gegenwart Dritter zu offenbaren (vgl. Tz. 4.8.4).

19. Seit Jahren erfolgten die Meldungen der Gesundheitsämter an den Beauftragten für die systematische Bekämpfung übertragbarer Krankheiten in personenbezogener Form. Nach unserer Intervention übermitteln die Gesundheitsämter diese Datensätze nur noch in anonymisierter Form.

20. In den Vernehmungsbögen der Polizei war nicht unterschieden, auf welche Fragen der Betroffene antworten muß, auf welche nicht. Die Formulare wurden nach unseren Vorschlägen überarbeitet. Künftig können Bürger ihr verfassungsmäßiges Recht, sich nicht selbst belasten zu müssen, besser wahrnehmen (vgl. Tz. 10.6).

21. Beim Bundeskriminalamt werden aufgrund von Meldungen der Länderpolizeien auf der Basis schwammiger Generalklauseln viele Daten über Personen mit Herkunft aus Osteuropa gespeichert. Das Innenministerium hat auf unsere Anregung hin ergänzende Regelungen erlassen, die sicherstellen, daß Meldungen erst erfolgen, wenn tatsächlich etwas gegen die Personen vorliegt.

22. Begehrte bisher ein Bürger Auskunft bei der Polizei über Daten, die in einem strafrechtlichen Ermittlungsverfahren gegen ihn erhoben worden waren, so mußte er damit rechnen, daß die Polizei die Auskunft ablehnte und auf die Staatsanwaltschaft verwies. In Zukunft wird auch die Polizei Auskünfte zu Datenspeicherungen in Ermittlungsverfahren geben.. Die Bürger erhalten damit direkt und unkompliziert Auskunft, welche Daten über sie gespeichert sind, ohne daß sie einen umständlichen Instanzenweg beschreiten müssen (vgl. Tz. 10.5).

23. Durch eine detaillierte Arbeitsanweisung hat der Verfassungsschutz nunmehr geregelt, in welchen Fällen eine Speicherung im Vorfeld extremistischer Betätigungen in Betracht kommt und in welchen nicht. Allein die Bekanntschaft mit den „falschen Leuten" führt nun nicht mehr zur Beobachtung durch den Verfassungsschutz (vgl. Tz. 10.10).

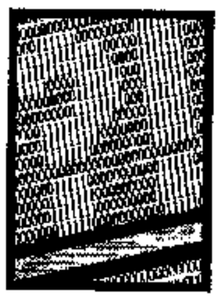
24. *Auf den in Justizvollzugsanstalten über die Gefangenen geführten Personalakten wurde bisher an vorderster Stelle ein Stempel aufgebracht, der unmittelbar auf eine Aids-Infektion der Gefangenen hindeutete. Das Justizministerium hat nun durch Erlaß festgelegt, daß die Information über die Aids-Infektion nur denjenigen Personen gegeben wird, die tatsächlich ansteckungsgefährdet sind (vgl. Tz. 10.13).*

25. *Bei der Geltendmachung von Schadensersatzansprüchen leitete das Finanzministerium bisher eine Vielzahl von personenbezogenen Daten über verletzte Justizbeamte an gewalttätige Gefangene weiter. Künftig werden nur noch die tatsächlich erforderlichen Informationen weitergegeben und zwar auch erst dann, wenn es unabdingbar ist. Die von Strafgefangenen verletzten Justizbeamten können jetzt darauf vertrauen, daß vor allem ihre Privatanschrift den Gefangenen auf diesem Wege nicht mehr offenbart wird (vgl. Tz. 4.4.5).*

26. *Die Jugendgerichtshilfe in einem Kreis speicherte bisher die Daten ihrer Probanden auch dann weiter, wenn das Verfahren gegen diese längst abgeschlossen war. Auf unsere Intervention wurden die Datenspeicherungen gelöscht. Diese Jugendlichen müssen künftig nicht mehr damit rechnen, daß ihre früheren Verfehlungen über die vom Gesetzgeber vorgesehenen Fristen gespeichert und auch nach Ablauf der Tilgungsfristen gegen sie verwandt werden.*

27. *In der Datenverarbeitung beim polizeilichen Staatsschutz waren die Grenzen zu den Kompetenzen des Verfassungsschutzes verwischt. In vielen Fällen waren Bürger nur deshalb gespeichert, weil sie Kontakt mit Verdächtigen hatten oder auch nur von ihrem demokratischen Recht auf Teilnahme an einer Demonstration Gebrauch gemacht hatten. Aufgrund unserer Beanstandungen werden diese Datenbestände umfassend bereinigt (vgl. Tz. 4.2.1).*

12. DATENSCHUTZAKADEMIE



Die DATENSCHUTZAKADEMIE hat ihr Jahresprogramm 1996 wie geplant abgewickelt. Einschließlich der Sonderkurse vor Ort wurden insgesamt 33 Kurse, Seminare und Workshops durchgeführt. Die ungebrochene Nachfrage nach dem Fortbildungsangebot der DATENSCHUTZAKADEMIE zeigt, daß in den öffentlichen Stellen des Landes ein großer Bedarf an Datenschutzberatung besteht. Insgesamt besuchten über 700 Teilnehmer unsere Veranstaltungen. In Teilen konnten wir nicht alle Wünsche erfüllen und mußten auf das Jahresprogramm 1997 vertrösten.

Das neue Jahresprogramm ist ein Kompromiß zwischen den Nachfragen und den begrenzten Möglichkeiten der Dienststelle. Insgesamt werden 30 Veranstaltungen zu 20 unterschiedlichen Themen angeboten. Neu sind Kurse zum „Datenschutz in Netzen“ und speziell für die Kommunalverwaltung. Neben den im Programm ausgedruckten Veranstaltungen wurden bereits eine Reihe von Sonderkursen vor Ort in verschiedenen Behörden terminiert.

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN

Kurse/Seminare/Workshops 1997

Kurse/Seminare/Workshops	**Kurzbez.**	**Zeit**	**Ort**
Datenschutz an der Schule	L 10	20.02.1997	Kiel
Datenschutzverordnung des Landes Schleswig-Holstein	VO 5	06.03.-07.03.1997	Leck
Einführungskurs für Schulsekretärinnen und Schulsekretäre	ES 2	20.03.1997	Bordesholm
Behördliche Datenschutzbeauftragte	D 7	21.04.-25.04.1997	Leck
Schutz von Personaldaten	P 4	06.05.-07.05.1997	Bordesholm
Datenschutz bei der Justiz	JD 1	12.05.-13.05.1997	Leck
Datenschutz im Ordnungsamt	O 3	14.05.-15.05.1997	Leck
Führung von Personalakten	PA 4	20.05.-21.05.1997	Bordesholm
Datenschutz an der Schule	L 11	22.05.1997	Kiel
Einstieg in das Datenschutzrecht	E 3	03.06.1997	Kiel
Datenschutz an der Schule	L 12	12.06.1997	Kiel
Einführungskurs Kommunalbereich	EK 1	17.06.1997	Kiel

Kurse/Seminare/Workshops	Kurzbez.	Zeit	Ort
Einführungskurs für Mitarbeiterinnen und Mitarbeiter von Verkehrsbehörden	EV 2	09.09.1997	Kiel
Schutz von Personaldaten	P 5	09.09.-10.09.1997	Bordesholm
Datenschutz an der Schule	L 13	11.09.1997	Kiel
Beauftragte für Sozialdatenschutz	S 5	15.09.-19.09.1997	Leck
Führung von Personalakten	PA 5	23.09.-24.09.1997	Bordesholm
Datenschutz im Bauamt	B 2	29.09.-30.09.1997	Leck
Datenschutz bei der Justiz	JSI 1	30.09.-01.10.1997	Leck
Personaldatenverarbeitung im Rahmen des Mitbestimmungsrechts	PR 3	01.10.-02.10.1997	Bordesholm
Datenschutz für Schulsekretärinnen und Schulsekretäre	ES 3	16.10.1997	Bordesholm
Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung	SI 3	20.10.-22.10.1997	Leck
Datenverarbeitungsrecht für Führungskräfte in der Verwaltung	F 6	23.10.-24.10.1997	Leck
Workshop für behördliche Datenschutzbeauftragte	DW 2	27.10.-28.10.1997	Leck
Einführungskurs Kommunalbereich	EK 2	11.11.1997	Kiel
Einführungskurs Datenschutz in Netzen	EN 1	18.11.1997	Kiel
Datenschutz im Bereich der Umweltverwaltung	U 3	24.11.-25.11.1997	Leck
Datenschutz bei der Justiz	JB 1	01.12.-02.12.1997	Leck
Workshop zur Datensicherheit	SIW 2	10.12.-11.12.1997	Leck
Datenschutz im Ordnungsamt	O 4	15.12.-16.12.1997	Leck

Das Jahresprogramm '97 der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN mit näheren Informationen zu den Veranstaltungen und Anmeldeformularen kann kostenlos angefordert werden

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

13. Sommerakademie 1997

SOMMER akademie'97

Am 25. August 1997 veranstaltet die DATENSCHUTZAKADEMIE im Landeshaus in Kiel die Sommerakademie 1997 zu folgendem Thema:

Computermedizin und Patientengeheimnis

Die älteste bekannte Datenschutzvorschrift ist der Eid des Hippokrates. Er verpflichtet den Arzt seit mehr als zweitausend Jahren, über das zu schweigen, was der Patient ihm anvertraut hat. Die Bedingungen der ärztlichen Heilbehandlung haben sich im Laufe der Zeit grundlegend geändert. Spezialisierung und Teamarbeit haben beispielsweise den Kreis derer immer größer werden lassen, denen der Patient seine Geheimnisse anvertraut. Gleichwohl blieb die Verschwiegenheitspflicht des Arztes, bei allen Änderungen im Detail, im Kern über die Jahrhunderte erhalten und findet sich heute in den ärztlichen Berufsordnungen und im Strafgesetzbuch wieder.

Die elektronische Datenverarbeitung, die heute in der Medizin eine immer größere Rolle spielt, hat gravierende Auswirkungen auf Inhalt und Reichweite der ärztlichen Verschwiegenheitspflicht. Wem vertraut der Patient seine Geheimnisse an, wenn Computer, von Softwarehäusern gewartet, selbsttätig Diagnosedaten erheben und speichern? Wer kann Kenntnis nehmen, wenn Krankheitsdaten im Rahmen der Telemedizin über tausende von Kilometern und dutzende von Knotenrechnern ausgetauscht werden? Ist die konventionelle Krankenakte sicherer zu handeln als eine hochkomplexe Datenbank? Sind die Patienten gut beraten, ihre Krankendaten besser selbst, z.B. auf einer Chipkarte, zu verwahren? Müssen wir es unter dem gegenwärtigen Kostendruck hinnehmen, daß die Krankenkassen über die Erkrankungen ihrer Versicherten immer besser Bescheid wissen? Und schließlich: Soll - und wenn ja, unter welchen Bedingungen - die medizinische Forschung Vorrang vor dem Patientengeheimnis haben?

Die Sommerakademie 1997 wird sich mit diesen Fragen auseinandersetzen. Ärzte, Techniker, Forscher, Juristen und Datenschützer haben Gelegenheit, über die Voraussetzungen zu diskutieren, unter denen auch im Computerzeitalter das Patientengeheimnis wirksam geschützt werden kann. Vorgesehen sind Vorträge, Diskussionen, praktische Vorführungen und Filmbeiträge.

Mitwirkende werden u.a. sein:

Dr. Hans Jürgen Ahrens; Landtagspräsident Heinz-Werner Arens; Dr. Bruno Baeriswyl; Ute Bertrand; Dr. Johann Bizer; Renate Harrington; Dr. Elmar H. Holler; Dr. Hans-Joachim Menzel; Ministerin Heide Moser; Prof. Dr. med. Otto Rienhoff; Horst Dieter Schirmer; Prof. Dr. Hans-Ludwig Schreiber; Prof. Dr. R. Trill; Reinhard Vetter; Dr. med. Dietrich Weisner; Dr. Rita Wellbrock; Dr. Helmut Bäumler.

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

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

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

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

Referat LD 1
Dr. Helmut Bäumler
App. 1200

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

Referat LD 2 **Eckhard Beilecke** App. 1205	
Jürgen von der Ohe App. 1206	Datenschutz im Bereich des Personal-, Wahl-, Melde-, Ausweis-, Ausländer-, Kommunal-, Gewerbe-, Bau- und Wirtschaftswesen Datenschutz im Bereich der Parlamentsverwaltung
Holger Brocks App. 1207	Datenschutz im Bereich des Statistik-, Verkehrs-, Umweltschutz-, Planungs-, Kataster-, 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
Heiko Behrendt App. 1212	Grundsatzfragen der Datensicherung und der ordnungsgemäßen Anwendung der DV-Programme (§§ 7, 8 LDSG) Prüfung von Rechenzentren
Thomas Lenz App. 1219	Prüfung von Behörden, soweit Fragen der automatisierten Datenverarbeitung berührt sind Mitwirkung bei der Erstellung von Gutachten EDV-Einsatz der Dienststelle
Referat LD 31 **Marit Köhntopp** App. 1214	Neue Medien und Informationstechniken, Medienrecht Technikfolgenabschätzung
Jan Ziegler App. 1213	Führung und Veröffentlichung der Dateienübersicht (§ 24 LDSG)

Referat LD 4	
Christina Ullrich App. 1215	
Gabriele Meyer-Bettyn App. 1216	Datenschutz im Sozial- und medizinischen Bereich
Referat LD 5	
Dr. Susanne Rublack App. 1204	Internationales Datenschutzrecht
Hans-Jürgen Strasdat App. 1217	Datenschutz im Polizei- und Verfassungsschutzbereich Datenschutz im Bereich der Staatsanwaltschaften
Silke Molt App. 1203	
Referat LD 51	
Lukas Gundermann App. 1204	Datenschutz im Justizbereich Recht der Neuen Medien

Beim **Landesbeauftragten für den Datenschutz** erhältliche Publikationen

Datenschutz in Schleswig-Holstein (13. Auflage)
Text des Landesdatenschutzgesetzes, der Datenschutzordnung
und des Bundesdatenschutzgesetzes mit einer erläuternden Einführung

Faltblätter „Hat der Bürger Rechte!?"
- Die Rechte des Bürgers im Datenschutz
- Was Sie über den Datenschutz wissen sollten
- Die Arbeit des Datenschutzbeauftragten
- Die Pflichten der datenverarbeitenden Stellen

Tätigkeitsberichte
der letzten drei Jahre als Landtagsdrucksache

Tätigkeitsberichte
als Sammlung

Diverse Aufkleber

DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN
- Broschüre
- Jahresprogramm 1997

Datenschutz auf Diskette
Der Landesbeauftragte für den Datenschutz hat eine Diskette herausgebracht, auf der die letzten fünf Tätigkeitsberichte, die Texte des Landesdatenschutzgesetzes und der Datenschutzverordnung sowie das Programm der DATENSCHUTZ-AKADEMIE gespeichert sind. Die Diskette kann beim Landesbeauftragten kostenlos angefordert werden. Das Programm ist benutzungsfreundlich gestaltet und leicht zu bedienen. Es erlaubt den beliebigen Wechsel zwischen Tätigkeitsberichten, Texten zitierter Paragraphen des Landesdatenschutzgesetzes oder der Datenschutzverordnung und dem Programm einschlägiger Kurse der DATENSCHUTZAKADEMIE. Als Systemvoraussetzung sind ein PC 386/486 oder höher, mindestens 4 MB Hauptspeicher, MS-DOS 5.0 aufwärts und Windows 3.1, Windows für Workgroups bzw. Windows 95/NT erforderlich.

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